

# NAT Gateway

# User Guide

**Issue** 01  
**Date** 2024-04-15



**Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2024. All rights reserved.**

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Cloud Computing Technologies Co., Ltd.

## **Trademarks and Permissions**



HUAWEI and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

## **Notice**

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

# Contents

|  |           |
|--|-----------|
| <b>1 Overview.....</b>   | <b>1</b>  |
| 1.1 What Is NAT Gateway?.....  | 1         |
| 1.2 Product Advantages.....  | 4         |
| 1.3 Scenarios.....   | 5         |
| 1.4 NAT Gateway Specifications.....  | 8         |
| 1.5 Constraints and Limitations.....   | 9         |
| 1.6 Permissions.....   | 10        |
| 1.7 Region and AZ.....   | 13        |
| 1.8 Basic Concepts.....  | 14        |
| <b>2 Getting Started.....</b>  | <b>16</b> |
| 2.1 Allowing a Private Network to Access the Internet Using SNAT.....                    | 16        |
| 2.1.1 Step 1: Assign an EIP.....   | 16        |
| 2.1.2 Step 2: Create a Public NAT Gateway.....   | 16        |
| 2.1.3 Step 3: Add an SNAT Rule.....  | 18        |
| 2.2 Allowing Internet Users to Access a Service in a Private Network Using DNAT.....     | 20        |
| 2.2.1 Overview.....  | 20        |
| 2.2.2 Step 1: Assign an EIP.....   | 21        |
| 2.2.3 Step 2: Create a Public NAT Gateway.....   | 21        |
| 2.2.4 Step 3: Add a DNAT Rule.....   | 23        |
| 2.2.5 Step 4: Test the Connection.....   | 25        |
| 2.3 Allowing On-Premises Servers to Communicate with the Internet.....                   | 26        |
| 2.3.1 Overview.....  | 26        |
| 2.3.2 Step 1: Connect Your On-premises Data Center to the Cloud with Direct Connect..... | 27        |
| 2.3.3 Step 2: Assign an EIP.....   | 27        |
| 2.3.4 Step 3: Create a Public NAT Gateway.....   | 27        |
| 2.3.5 Step 4: Add an SNAT Rule.....  | 29        |
| 2.3.6 Step 5: Add a DNAT Rule.....   | 31        |
| <b>3 Public NAT Gateways.....</b>  | <b>33</b> |
| 3.1 Public NAT Gateway Overview.....   | 33        |
| 3.2 Managing Public NAT Gateways.....  | 34        |
| 3.2.1 Creating a Public NAT Gateway.....   | 34        |
| 3.2.2 Viewing a Public NAT Gateway.....  | 36        |

|   |           |
|---|-----------|
| 3.2.3 Modifying a Public NAT Gateway.....                 | 36        |
| 3.2.4 Deleting a Public NAT Gateway.....                  | 37        |
| 3.3 Managing SNAT Rules.....                              | 37        |
| 3.3.1 Adding an SNAT Rule.....                            | 38        |
| 3.3.2 Viewing an SNAT Rule.....                           | 39        |
| 3.3.3 Deleting an SNAT Rule.....                          | 40        |
| 3.4 Managing DNAT Rules.....                              | 40        |
| 3.4.1 Adding a DNAT Rule.....                             | 40        |
| 3.4.2 Viewing a DNAT Rule.....                            | 43        |
| 3.4.3 Modifying a DNAT Rule.....                          | 43        |
| 3.4.4 Deleting a DNAT Rule.....                           | 43        |
| 3.4.5 Deleting DNAT Rules in Batches.....                 | 44        |
| <b>4 Private NAT Gateways.....</b>                        | <b>45</b> |
| 4.1 Private NAT Gateway Overview.....                     | 45        |
| 4.2 Creating a Private NAT Gateway.....                   | 46        |
| 4.2.1 Overview.....                                       | 46        |
| 4.2.2 Creating a Private NAT Gateway.....                 | 47        |
| 4.2.3 Assigning a Transit IP Address.....                 | 49        |
| 4.2.4 Adding an SNAT Rule.....                            | 49        |
| 4.2.5 Adding a DNAT Rule.....                             | 50        |
| 4.3 Managing Private NAT Gateways.....                    | 53        |
| 4.3.1 Viewing a Private NAT Gateway.....                  | 53        |
| 4.3.2 Modifying a Private NAT Gateway.....                | 53        |
| 4.3.3 Deleting a Private NAT Gateway.....                 | 54        |
| 4.4 Managing SNAT Rules.....                              | 54        |
| 4.4.1 Viewing an SNAT Rule.....                           | 54        |
| 4.4.2 Modifying an SNAT Rule.....                         | 55        |
| 4.4.3 Deleting an SNAT Rule.....                          | 55        |
| 4.5 Managing DNAT Rules.....                              | 56        |
| 4.5.1 Viewing a DNAT Rule.....                            | 56        |
| 4.5.2 Modifying a DNAT Rule.....                          | 56        |
| 4.5.3 Deleting a DNAT Rule.....                           | 57        |
| 4.6 Managing Transit Subnets.....                         | 57        |
| 4.6.1 Creating a Transit Subnet.....                      | 57        |
| 4.6.2 Viewing a Transit Subnet.....                       | 58        |
| 4.6.3 Modifying a Transit Subnet.....                     | 59        |
| 4.6.4 Deleting a Transit Subnet.....                      | 59        |
| 4.7 Managing Transit IP Addresses.....                    | 60        |
| 4.7.1 Assigning a Transit IP Address.....                 | 60        |
| 4.7.2 Viewing a Transit IP Address.....                   | 61        |
| 4.7.3 Releasing a Transit IP Address.....                 | 61        |
| 4.8 Accessing On-Premises Data Centers or Other VPCs..... | 61        |

|  |           |
|--|-----------|
| <b>5 Permissions Management</b>  | <b>63</b> |
| 5.1 Creating a User and Granting NAT Gateway Permissions   | 63        |
| 5.2 NAT Gateway Custom Policies  | 64        |
| <b>6 Monitoring</b>  | <b>67</b> |
| 6.1 Supported Metrics  | 67        |
| 6.2 Viewing Metrics  | 69        |
| <b>7 FAQs</b>  | <b>71</b> |
| 7.1 Public NAT Gateways  | 71        |
| 7.1.1 What Is the Relationship Between a VPC, Public NAT Gateway, EIP Bandwidth, and ECS?                        | 71        |
| 7.1.2 How Does a Public NAT Gateway Offer High Availability?   | 71        |
| 7.2 Private NAT Gateways   | 71        |
| 7.2.1 How Do I Troubleshoot a Network Failure After a Private NAT Gateway Is Configured?                         | 71        |
| 7.2.2 How Many Private NAT Gateways Can I Create in a VPC?   | 72        |
| 7.2.3 Can an SNAT Rule and a DNAT Rule of a Private NAT Gateway Share the Same Transit IP Address?               | 72        |
| 7.2.4 Can Private NAT Gateways Translate On-premises IP Addresses Connected to the Cloud Through Direct Connect? | 72        |
| 7.2.5 What Are the Differences Between Private NAT Gateways and Public NAT Gateways?                             | 73        |
| 7.2.6 Can a Private NAT Gateway Be Used Across Accounts?   | 73        |
| 7.3 SNAT Rules   | 73        |
| 7.3.1 Why Do I Need SNAT?  | 73        |
| 7.3.2 What Are SNAT Connections?   | 73        |
| 7.4 DNAT Rules   | 74        |
| 7.4.1 Why Do I Need DNAT?  | 74        |
| 7.4.2 Can I Modify DNAT Rules?   | 74        |
| <b>A Change History</b>  | <b>75</b> |

# 1 Overview

---

## 1.1 What Is NAT Gateway?

NAT Gateway is a network address translation (NAT) service. It can be a public NAT gateway or a private NAT gateway.

### Public NAT Gateways

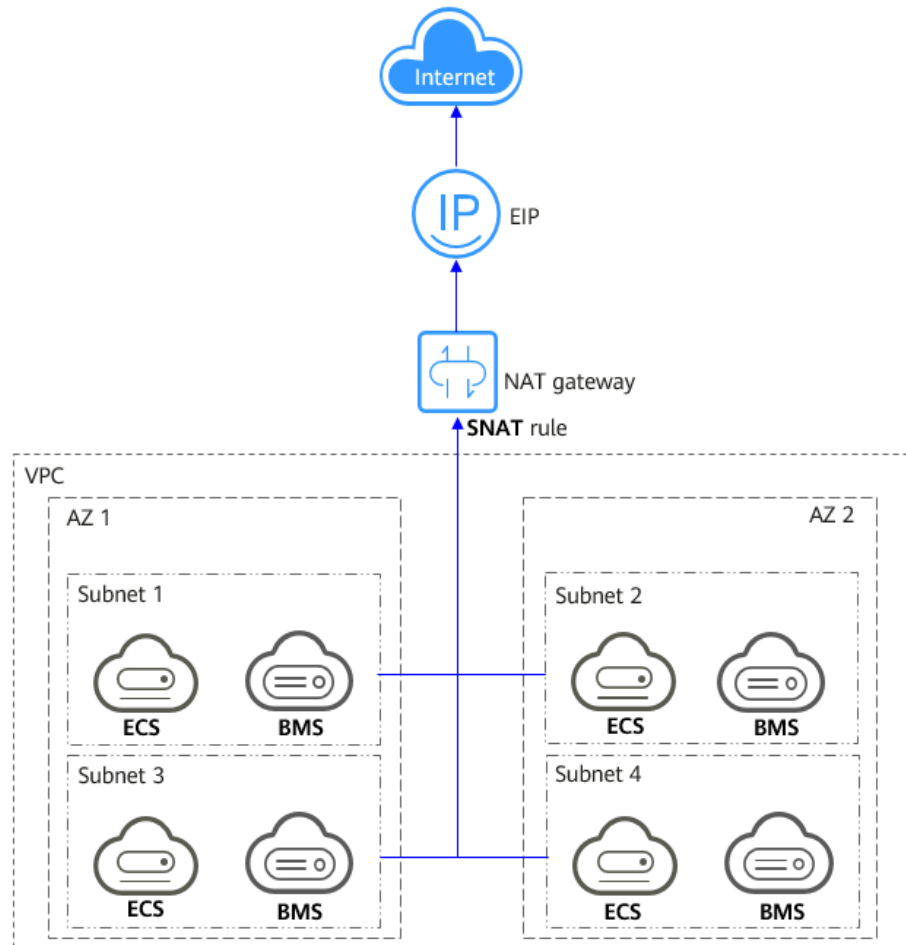
A public NAT gateway enables cloud and on-premises servers in a private subnet to share an EIP to access the Internet or provide services accessible from the Internet. Cloud servers are ECSs and BMSs in a VPC. On-premises servers are servers in on-premises data centers that connect to a VPC through Direct Connect or Virtual Private Network (VPN). A public NAT gateway supports up to 20 Gbit/s of bandwidth.

Public NAT gateways offer source NAT (SNAT) and destination NAT (DNAT).

- SNAT translates private IP addresses into EIPs so that traffic from a private network can go out to the Internet.

**Figure 1-1** shows how an SNAT rule works.

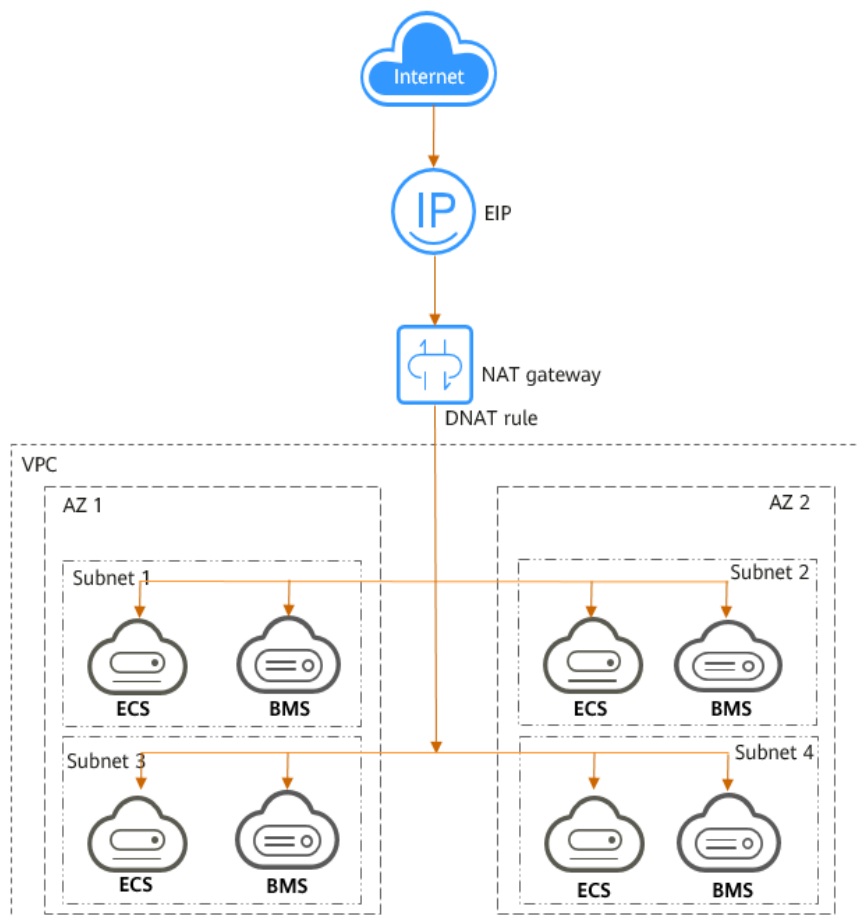
Figure 1-1 NAT gateway with an SNAT rule



- DNAT enables servers within an AZ or across AZs in a VPC to share an EIP to provide services accessible from the Internet. With an EIP, a NAT gateway forwards the Internet requests from only a specific port and over a specific protocol to a specific port of a server, or it can forward all requests to the server regardless of which port they originated on.

Figure 1-2 shows how a DNAT rule works.

Figure 1-2 NAT gateway with a DNAT rule



## Private NAT Gateways

Private NAT gateways provide network address translation, allowing ECSs and BMSs in a VPC to communicate with servers in other VPCs or on-premises data centers. You can configure SNAT and DNAT rules for a NAT gateway to translate the source and destination IP addresses of originating packets into a transit IP address.

Specifically,

- SNAT enables servers within one AZ or across AZs in a VPC to share a transit IP address to access on-premises data centers or other VPCs.
- DNAT enables servers that share the same transit IP address in a VPC to provide services accessible from on-premises data centers or other VPCs.

### Transit Subnet

A transit subnet is a transit network and is the subnet to which the transit IP address belongs.

### Transit IP Address

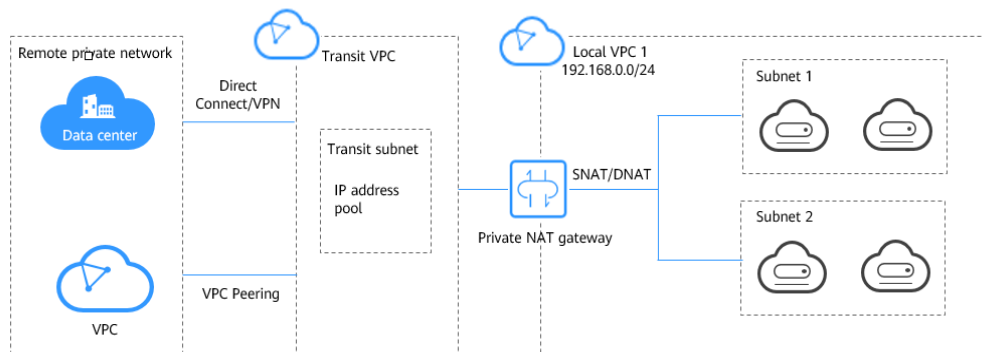
A transit IP address is a private IP address that can be assigned from a transit subnet. Cloud servers in your VPC can share a transit IP address to access on-premises networks or other VPCs.



## Transit VPC

A transit VPC is where a transit subnet belongs to.

**Figure 1-3** Private NAT gateway



## How Do I Access the NAT Gateway Service?

You can access the NAT Gateway service through the management console or using HTTPS-based APIs.

- **Management console**  
Log in to the management console and choose **NAT Gateway** from the service list.
- **APIs**  
If you need to integrate NAT Gateway on the cloud platform into your own system, use APIs to access NAT Gateway.

## 1.2 Product Advantages

### Advantages of Public NAT Gateways

- **Flexible deployment**  
A NAT gateway can be shared across subnets and AZs, so that even if an AZ fails, the public NAT gateway can still run normally in another AZ. The specifications and EIP of a public NAT gateway can be changed at any time.
- **Ease of use**  
Multiple NAT gateway specifications are available. Public NAT gateway configuration is simple, the operation & maintenance is easy, and they can be provisioned quickly. Once provisioned, they can run stably.
- **Cost-effectiveness**  
Servers can share one EIP to connect to the Internet. You no longer need to configure one EIP for each server, which saves money on EIPs and bandwidth.

### Advantages of Private NAT Gateways

- **Easier network planning**

Different departments in a large enterprise may have overlapping CIDR blocks, so the enterprise has to replan its network before migrating their workloads to the cloud. The replanning is time-consuming and stressful. The private NAT gateway eliminates the need to replan the network so that customers can retain their original network while migrating to the cloud.

- **Easy operation & maintenance**

Departments of a large enterprise usually have hierarchical networks for hierarchical organizations, rights- and domain-based management, and security isolation. Such hierarchical networks need to be mapped to a large-scale network for enabling communication between them. A private NAT gateway can map the CIDR block of each department to the same VPC CIDR block, which simplifies the management of complex networks.

- **Strong security**

Departments of an enterprise may need different levels of security. Private NAT gateways can expose the IP addresses and ports of only specified CIDR blocks to meet high security requirements. An industry regulation agency may require other organizations to use a specified IP address to access their regulation system. Private NAT gateways can help meet this requirement by mapping private IP addresses to that specified IP address.

- **Zero IP conflicts**

Isolated services of multiple departments usually use IP addresses from the same private CIDR block. After the enterprise migrates workloads to the cloud, IP address conflicts occur. Thanks to IP address mapping, the private NAT gateways allow for communication between overlapping CIDR blocks.

## 1.3 Scenarios

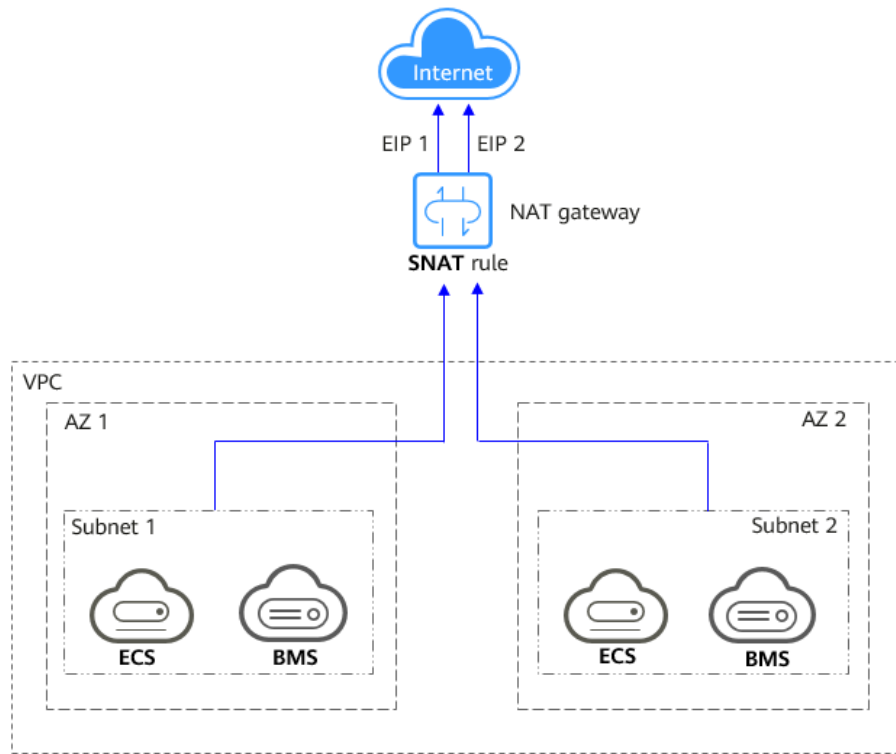
### Public NAT Gateway

- **Allowing a private network to access the Internet using SNAT**

If your servers in a VPC need to access the Internet, you can configure SNAT rules to let these servers use EIPs to access the Internet without exposing their private IP addresses. You can configure only one SNAT rule for each subnet in a VPC, and select one or more EIPs for each SNAT rule. Public NAT Gateway provides different numbers of connections, and you can create multiple SNAT rules to meet your service requirements.

**Figure 1-4** shows how servers in a VPC access the Internet using SNAT.

**Figure 1-4** Allowing a private network to access the Internet using SNAT



- **Allowing Internet users to access a service in a private network using DNAT**

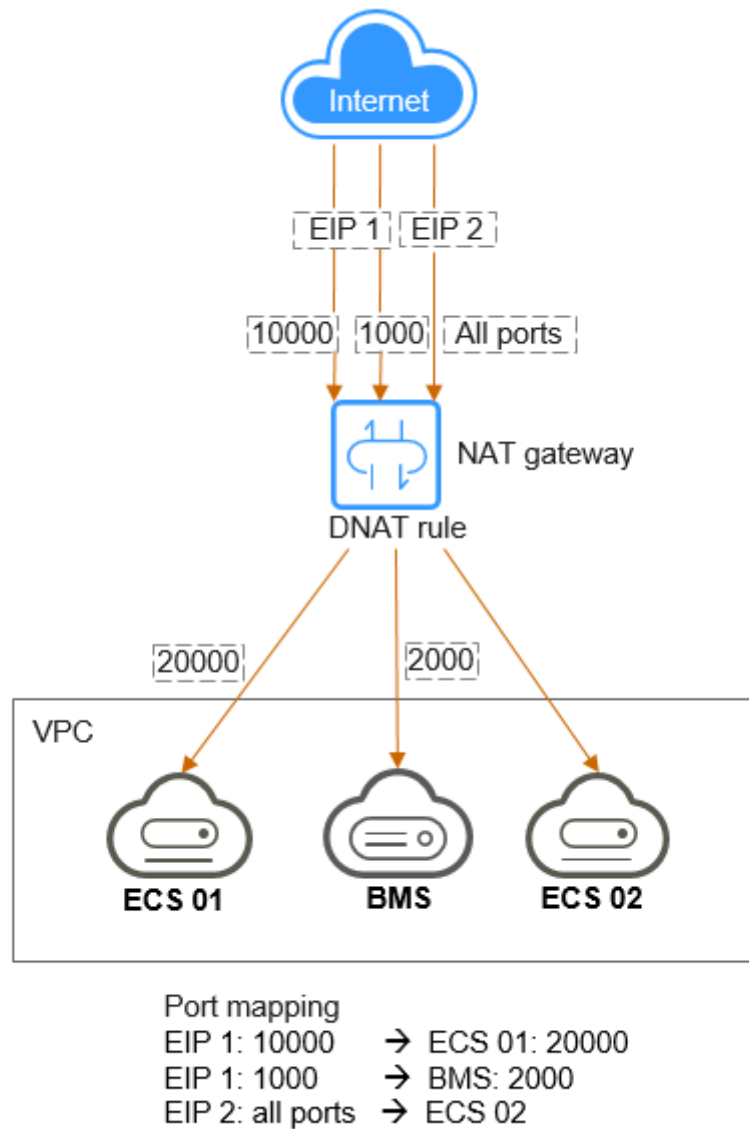
DNAT rules enable servers in a VPC to provide services accessible from the Internet.

After receiving requests from a specific port over a specific protocol, the public NAT gateway can forward the requests to a specific port of a server through port mapping. The public NAT gateway can also forward all requests destined for an EIP to a specific server through IP address mapping.

One DNAT rule can be configured for each server. If there are multiple servers, you can create multiple DNAT rules to map one or more EIPs to the private IP addresses of these servers.

**Figure 1-5** shows how servers (ECSs or BMSs) in a VPC provide services accessible from the Internet using DNAT.

**Figure 1-5** Allowing Internet users to access a service in a private network using DNAT

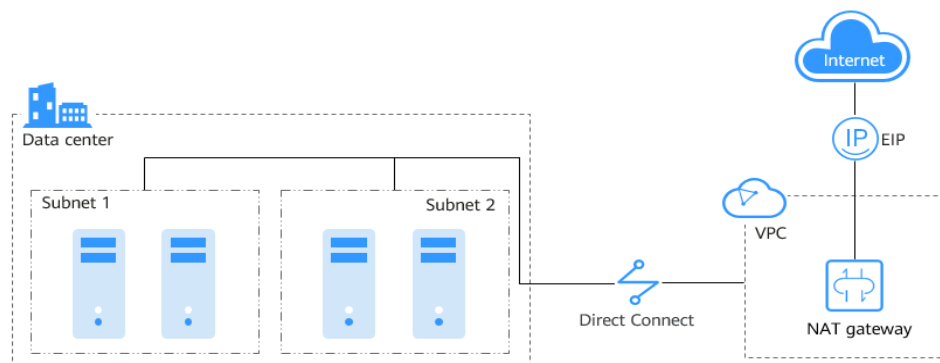


- **Allowing on-premises servers to communicate with the Internet**

In certain Internet, gaming, e-commerce, and financial scenarios, a large number of servers in a private cloud are connected to a VPC through Direct Connect or VPN. If such servers need secure, high-speed Internet access or need to provide services accessible from the Internet, you can deploy a NAT gateway and configure SNAT and DNAT rules to meet their requirements.

**Figure 1-6** shows how to use SNAT and DNAT to provide high-speed Internet access or provide services accessible from the Internet.

**Figure 1-6** Allowing on-premises servers to communicate with the Internet



## 1.4 NAT Gateway Specifications

The NAT gateway performance is determined by the maximum number of SNAT connections supported.

### Public NAT Gateway

An SNAT connection consists of a source IP address, source port, destination IP address, destination port, and a transport layer protocol. The source IP address is the EIP, and the source port is the EIP port. An SNAT connection uniquely identifies a session.

Throughput is the total bandwidth of all EIPs in DNAT rules. For example, a public NAT gateway has two DNAT rules. The EIP bandwidth in the first DNAT rule is 10 Mbit/s, and that in the second DNAT rule is 5 Mbit/s. The throughput of the public NAT gateway will be 15 Mbit/s.

Select a public NAT gateway based on your service requirements. [Table 1-1](#) lists the public NAT gateway specifications.

**Table 1-1** Public NAT gateway specifications

| Specifications | Maximum Number of SNAT Connections | Bandwidth |
|----------------|------------------------------------|-----------|
| Small          | 10,000                             | 20 Gbit/s |
| Medium         | 50,000                             | 20 Gbit/s |
| Large          | 200,000                            | 20 Gbit/s |
| Extra-large    | 1,000,000                          | 20 Gbit/s |

## Private NAT Gateway

An SNAT connection consists of a source IP address, source port, destination IP address, destination port, and a transport layer protocol. The source IP address is the transit IP address, and the source port is the port of the transit IP address.

Select a private NAT gateway based on your service requirements. [Table 1-2](#) lists the private NAT gateway specifications.

**Table 1-2** Private NAT gateway specifications

| Specifications | Maximum Number of SNAT Connections | Bandwidth  |
|----------------|------------------------------------|------------|
| Small          | 2,000                              | 200 Mbit/s |
| Medium         | 5,000                              | 500 Mbit/s |
| Large          | 20,000                             | 2 Gbit/s   |
| Extra-large    | 50,000                             | 5 Gbit/s   |

### NOTE

If the number of requests exceeds the maximum allowed connections of a private NAT gateway, services will be adversely affected. To avoid this situation, create alarm rules on the Cloud Eye console to monitor the number of SNAT connections.

## 1.5 Constraints and Limitations

### Public NAT Gateway

When using a public NAT gateway, note the following:

- Common restrictions
  - Rules on one public NAT gateway can use the same EIP, but rules on different NAT gateways must use different EIPs.
  - Each VPC can have only one NAT gateway.
  - SNAT and DNAT rules cannot use the same EIP.
  - If both an EIP and a public NAT gateway are configured for a server, data will be forwarded through the EIP.
  - NAT Gateway supports TCP, UDP, and ICMP, but does not support application layer gateway (ALG)-related technologies. In addition, NAT Gateway does not support Encapsulating Security Payload (ESP) and Authentication Header (AH) used by Generic Routing Encapsulation (GRE) tunnels and Internet Protocol Security (IPsec). This is determined by the features of NAT Gateway.
- SNAT restrictions
  - Only one SNAT rule can be added for each VPC subnet.

- When you add an SNAT rule in the VPC scenario, the custom CIDR block must be a subset of the NAT gateway's VPC subnets.
- If an SNAT rule is used in the Direct Connect scenario, the custom CIDR block must be a CIDR block of a Direct Connect connection and cannot overlap with the NAT gateway's VPC subnets.
- There is no limit on the number of SNAT rules that can be added on a public NAT gateway.
- DNAT restrictions
  - DNAT rules cannot map virtual IP addresses to EIPs.
  - Only one DNAT rule can be configured for each port on a server. One port can be mapped to only one EIP.
  - A maximum of 200 DNAT rules can be added on a public NAT gateway.

## Private NAT Gateway

When using a private NAT gateway, note the following:

- Common restrictions
  - Manually add routes in a VPC to connect it to a remote private network through a VPC peering connection, Direct Connect, or VPN connection.
  - The transit IP address and destination IP address cannot be in the same VPC.
  - SNAT and DNAT rules cannot share a transit IP address.
  - The total number of DNAT and SNAT rules that can be added on a private NAT gateway varies with the private NAT gateway specifications.
    - Small: 20 or less
    - Medium: 50 or less
    - Large: 200 or less
    - Extra-large: 500 or less
- SNAT restrictions
  - Only one SNAT rule can be added for each VPC subnet.
- DNAT restrictions
  - A DNAT rule with **Port Type** set to **All ports** cannot share a transit IP address with a DNAT rule with **Port Type** set to **Specific port**.

## 1.6 Permissions

You can use Identity and Access Management (IAM) to manage NAT Gateway permissions and control access to your resources. IAM provides identity authentication, permissions management, and access control.

With IAM, you can create IAM users and assign permissions to control their access to specific resources. For example, you can create IAM users for software developers and assign specific permissions to allow them to use NAT Gateway resources but prevent them from being able to delete resources or perform any high-risk operations.

If your account does not require individual IAM users for permissions management, you can skip this section.

IAM is a free service. You only pay for the resources in your account. For more information about IAM, see *Identity and Access Management User Guide*.

## NAT Gateway Permissions

New IAM users do not have any permissions assigned by default. You need to first add them to one or more groups and attach policies or roles to these groups. The users then inherit permissions from the groups and can perform specified operations on cloud services based on the permissions they have been assigned.

NAT Gateway is a project-level service deployed and accessed in specific physical regions. When assigning NAT Gateway permissions to a user group, specify region-specific projects where the permissions will take effect. If you select **All projects**, the permissions will be granted for all region-specific projects. When accessing NAT Gateway, the users need to switch to a region where they have been authorized to use this service.

You can grant users permissions by using roles and policies.

- **Roles:** A type of coarse-grained authorization mechanism that provides only a limited number of service-level roles. When using roles to grant permissions, you also need to assign dependency roles. However, roles are not an ideal choice for fine-grained authorization and secure access control.
- **Policies:** A type of fine-grained authorization mechanism that defines permissions required to perform operations on specific cloud resources under certain conditions. This mechanism allows for more flexible policy-based authorization for more secure access control. For example, the account administrator can grant users only permission to manage a certain type of NAT gateways and SNAT rules. Most policies define permissions based on APIs. For the API actions supported by NAT Gateway, see section "Permissions Policies and Supported Actions" in the *NAT Gateway API Reference*.

**Table 1-3** lists all the system-defined roles and policies supported by NAT Gateway.

**Table 1-3** System-defined roles and policies supported by NAT Gateway

| Policy Name        | Description   | Type                  |
|--------------------|---|-----------------------|
| NAT FullAccess     | All operations on NAT Gateway resources.  | System-defined policy |
| NAT ReadOnlyAccess | Read-only permissions for all NAT Gateway resources.  | System-defined policy |
| NAT Administrator  | All operations on NAT Gateway resources. To be granted this permission, users must also have the <b>Tenant Guest</b> permissions. | System-defined role   |

**Table 1-4** lists the common operations supported by each NAT Gateway system policy or role. Select the policies or roles as required.



**Table 1-4** Common operations supported by each system-defined policy or role of NAT Gateway

| Operation                               | NAT FullAccess | NAT ReadOnlyAccess | NAT Gateway Administrator |
|---|----------------|--------------------|---------------------------|
| Creating a NAT gateway                  | √              | x                  | √                         |
| Querying NAT gateways                   | √              | √                  | √                         |
| Querying NAT gateway details            | √              | √                  | √                         |
| Updating a NAT gateway                  | √              | x                  | √                         |
| Deleting a NAT gateway                  | √              | x                  | √                         |
| Adding an SNAT rule                     | √              | x                  | √                         |
| Viewing an SNAT rule                    | √              | √                  | √                         |
| Modifying an SNAT rule                  | √              | x                  | √                         |
| Deleting an SNAT rule                   | √              | x                  | √                         |
| Adding a DNAT rule                      | √              | x                  | √                         |
| Viewing a DNAT rule                     | √              | √                  | √                         |
| Modifying a DNAT rule                   | √              | x                  | √                         |
| Deleting a DNAT rule                    | √              | x                  | √                         |
| Creating a transit subnet               | √              | x                  | √                         |
| Querying transit subnets                | √              | √                  | √                         |
| Querying details about a transit subnet | √              | √                  | √                         |
| Modifying a transit subnet              | √              | x                  | √                         |

| Operation                      | NAT FullAccess | NAT ReadOnlyAccess | NAT Gateway Administrator |
|--------------------------------|----------------|--------------------|---------------------------|
| Deleting a transit subnet      | √              | x                  | √                         |
| Assigning a transit IP address | √              | x                  | √                         |
| Querying a transit IP address  | √              | √                  | √                         |
| Releasing a transit IP address | √              | x                  | √                         |

 NOTE

- Note the following when creating a DNAT rule:
  - If you set **Instance Type** to **Server** and select an ECS, you also need to obtain the **ECS ReadOnlyAccess** permissions or the fine-grained permissions for actions **ecs:cloudServers:get** and **ecs:cloudServers:list**. For details, see the *Elastic Cloud Server API Reference*.
  - If you set **Instance Type** to **Server** and select a BMS, you also need to obtain the **BMS ReadOnlyAccess** permissions or the fine-grained permissions for actions **bms:servers:get** and **bms:servers:list**. For details, see the *Bare Metal Server API Reference*.
  - If you create a DNAT rule on a private NAT gateway and select **Load balancer** for **Instance Type**, you need to obtain the **ELB ReadOnlyAccess** permissions or the fine-grained permissions for actions **elb:loadbalancers:get** and **elb:loadbalancers:list**. For details, see the *Elastic Load Balance API Reference*.
  - After a DNAT rule is created, add a security group rule to allow the Internet to access servers for which the DNAT rule is configured. Otherwise, the DNAT rule does not take effect. Obtain the **VPC FullAccess** permissions or the fine-grained permissions for action **vpc:securityGroups:create** by referring to the *Virtual Private Cloud API Reference*.
- To view metrics, obtain the **CES ReadOnlyAccess** permissions. For details, see the *Cloud Eye API Reference*.
- To view access logs, obtain the **LTS ReadOnlyAccess** permissions. For details, see the *Log Tank Service API Reference*.

## Helpful Links

- [Creating a User and Granting NAT Gateway Permissions](#)

## 1.7 Region and AZ

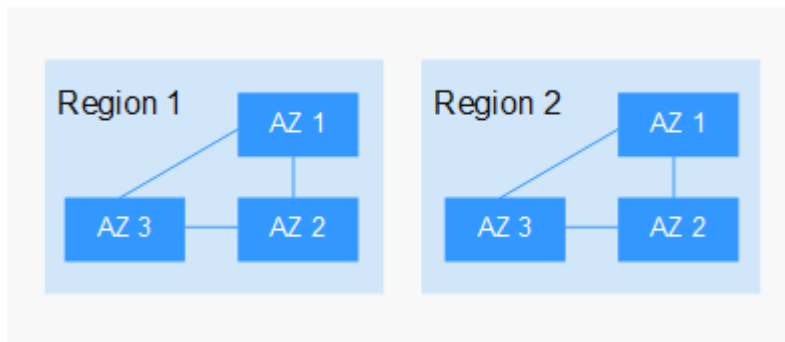
### Concept

A region and availability zone (AZ) identify the location of a data center. You can create resources in a specific region and AZ.

- A region is a physical data center, which is completely isolated to improve fault tolerance and stability. The region that is selected during resource creation cannot be changed after the resource is created.
- An AZ is a physical location where resources use independent power supplies and networks. A region contains one or more AZs that are physically isolated but interconnected through internal networks. Because AZs are isolated from each other, any fault that occurs in one AZ will not affect others.

**Figure 1-7** shows the relationship between regions and AZs.

**Figure 1-7** Regions and AZs



## Selecting a Region

Select a region closest to your target users for lower network latency and quick access.

## Selecting an AZ

When deploying resources, consider your applications' requirements on disaster recovery (DR) and network latency.

- For high DR capability, deploy resources in different AZs within the same region.
- For lower network latency, deploy resources in the same AZ.

## Regions and Endpoints

Before you use an API to call resources, specify its region and endpoint. For more details, see [Regions and Endpoints](#).

# 1.8 Basic Concepts

## EIP

An EIP is a static, public IP address.

An EIP can be directly accessed over the Internet. A private IP address is an IP address on a local area network (LAN) and cannot be routed through the Internet.

You can bind an EIP to an ECS in your subnet to enable the ECS to communicate with the Internet.

Each EIP can be used by only one ECS at a time. To enable servers across AZs in a VPC to share an EIP, use a NAT gateway.

## **SNAT Connections**

An SNAT connection consists of a source IP address, source port, destination IP address, destination port, and a transport layer protocol. The source IP address is the EIP, and the source port is the EIP port. An SNAT connection uniquely identifies a session.

## **DNAT Connections**

DNAT connections enable servers in a private network to share an EIP to provide services accessible from the Internet.

# 2 Getting Started

---

## 2.1 Allowing a Private Network to Access the Internet Using SNAT

### 2.1.1 Step 1: Assign an EIP

#### Scenarios

You can assign an EIP for your public NAT gateway so that servers in a VPC can use this EIP to access the Internet.

#### Procedure

For details, see the *Elastic IP User Guide*.

You do not need to bind the EIP to any server.

### 2.1.2 Step 2: Create a Public NAT Gateway

#### Scenarios

a public NAT gateway to enable your servers to access the Internet or provide services accessible from the Internet.

#### Prerequisites

- The VPC and subnet where your public NAT gateway will be deployed are available.
- To allow traffic to pass through the public NAT gateway, a route to the public NAT gateway in the VPC is required. When you create a public NAT gateway, a default route 0.0.0.0/0 to the public NAT gateway is automatically added to the default route table of the VPC. If the default route 0.0.0.0/0 already exists in the default route table of the VPC before you create the public NAT gateway, the default route that points to the public NAT gateway will fail to

be added automatically. In this case, perform the following operations after the public NAT gateway is successfully created: Manually add a different route that points to the gateway or create a default route 0.0.0.0/0 pointing to the gateway in the new routing table.

## Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.  
The **Public NAT Gateway** page is displayed.
3. On the displayed page, click **Create Public NAT Gateway**.
4. Configure required parameters. For details, see [Table 2-1](#).

**Table 2-1** Descriptions of public NAT gateway parameters

| Parameter | Description  |
|-----------|--|
| Region    | The region where the public NAT gateway is located   |
| Name      | The name of the public NAT gateway<br>Enter up to 64 characters. Only digits, letters, underscores (_), hyphens (-), and periods (.) are allowed.  |
| VPC       | The VPC that the public NAT gateway belongs to<br>The selected VPC cannot be changed after you create the public NAT gateway.<br><b>NOTE</b><br>To allow traffic to pass through the public NAT gateway, a route to the public NAT gateway in the VPC is required. When you create a public NAT gateway, a default route 0.0.0.0/0 to the public NAT gateway is automatically added to the default route table of the VPC. If the default route 0.0.0.0/0 already exists in the default route table of the VPC before you create the public NAT gateway, the default route that points to the public NAT gateway will fail to be added automatically. In this case, perform the following operations after the public NAT gateway is successfully created: Manually add a different route that points to the gateway or create a default route 0.0.0.0/0 pointing to the gateway in the new routing table. |
| Subnet    | The subnet that the public NAT gateway belongs to<br>The subnet must have at least one available IP address.<br>The selected subnet cannot be changed after you create the public NAT gateway.<br>The NAT gateway will be deployed in the selected subnet. The NAT gateway works for the entire VPC where it is deployed. To enable communications over the Internet, add SNAT or DNAT rules.  |

| Parameter      | Description  |
|----------------|--|
| Specifications | The specifications of the public NAT gateway<br>The value can be <b>Extra-large, Large, Medium, or Small</b> . To view more details about specifications, click <b>Learn more</b> on the page. |
| Description    | Supplementary information about the public NAT gateway<br>Enter up to 255 characters. Angle brackets (<>) are not allowed.   |

5. Click **Create Now**. On the page displayed, confirm the public NAT gateway specifications.
6. Click **Submit**.  
It takes 1 to 6 minutes to create a public NAT gateway.
7. In the list, view the status of the public NAT gateway.

 **NOTE**

After the public NAT gateway is created, check whether a default route (0.0.0.0/0) that points to the public NAT gateway exists in the default route table of the VPC where the public NAT gateway is. If no, add a route pointing to the public NAT gateway to the default route table, alternatively, create a custom route table and add the default route 0.0.0.0/0 pointing to the public NAT gateway to the table. The following describes how to add a route to a custom route table.

## Adding a Default Route Pointing to the Public NAT Gateway

1. Log in to the management console.
2. Under **Network**, select **Virtual Private Cloud**.
3. In the navigation pane on the left, choose **Route Tables**.
4. On the **Route Tables** page, click **Create Route Table** in the upper right corner.  
**VPC:** Select the VPC to which the public NAT gateway belongs.
5. After the custom route table is created, click its name.  
The **Summary** page is displayed.
6. Click **Add Route** and configure parameters as follows:  
**Destination:** Set it to **0.0.0.0/0**.  
**Next Hop Type:** Select **NAT gateway**.  
**Next Hop:** Select the created NAT gateway.
7. Click **OK**.

## 2.1.3 Step 3: Add an SNAT Rule

### Scenarios

After creating a public NAT gateway, add an SNAT rule to enable your servers in a specific subnet to access the Internet through the same EIP.

One SNAT rule can be configured for only one subnet or CIDR block. If there are multiple subnets or CIDR blocks in a VPC, you can add multiple SNAT rules to allow servers to share EIPs.

## Prerequisites

A public NAT gateway is available.

## Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.  
The **Public NAT Gateway** page is displayed.
3. On the displayed page, click the name of the public NAT gateway on which you need to add an SNAT rule.
4. On the **SNAT Rules** tab, click **Add SNAT Rule**.
5. Configure required parameters. [Table 2-2](#) describes the parameters.

**Table 2-2** Descriptions of SNAT rule parameters

| Parameter  | Description   |
|------------|---|
| Scenario   | Select <b>VPC</b> if your servers in a VPC will use the SNAT rule to access the Internet.   |
| Subnet     | The subnet in which servers can use the SNAT rule to access the Internet <ul style="list-style-type: none"> <li>● <b>Existing</b>: Select an existing subnet.</li> <li>● <b>Custom</b>: Customize a CIDR block or enter a server IP address.</li> </ul> <p><b>NOTE</b><br/>The customized CIDR block must be a subset of the VPC subnet CIDR block. You can configure a 32-bit host IP address. The NAT gateway takes effect only for this address.</p> |
| CIDR Block | The CIDR block is a subset of the NAT gateway's VPC subnets<br>Servers whose IP addresses in the CIDR block can use the SNAT rule to access the Internet.   |
| EIP        | The EIP used for accessing the Internet<br>You can select an EIP that either has not been bound, has been bound to a DNAT rule of the current public NAT gateway with <b>Port Type</b> set to <b>Specific port</b> , or has been bound to an SNAT rule of the current public NAT gateway.   |
| Monitoring | You can create alarm rules on the Cloud Eye console to monitor your SNAT connections and keep informed of any changes in a timely manner.   |



| Parameter   | Description  |
|-------------|--|
| Description | Provides supplementary information about the SNAT rule. Enter up to 255 characters. Angle brackets (<>) are not allowed. |

6. Click **OK**.

**NOTE**

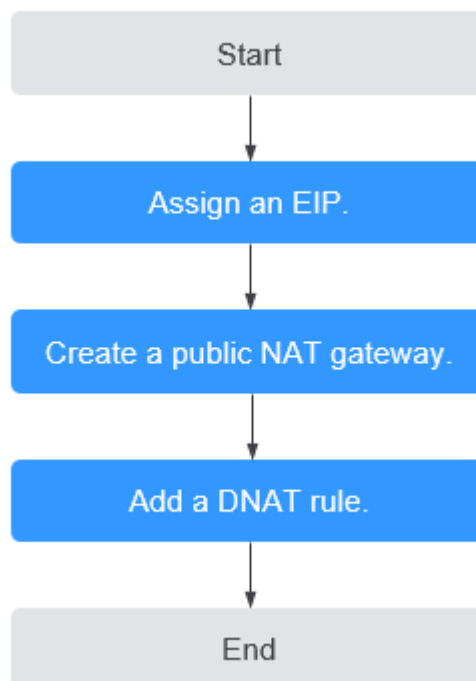
- You can add multiple SNAT rules for a public NAT gateway to suite your service requirements.
- Only one SNAT rule can be added for each VPC subnet.

## 2.2 Allowing Internet Users to Access a Service in a Private Network Using DNAT

### 2.2.1 Overview

When one or more servers (ECSs and BMSs) in a VPC need to provide services accessible from the Internet, you can add DNAT rules.

**Figure 2-1** Flowchart



## 2.2.2 Step 1: Assign an EIP

### Scenarios

You can buy an EIP for your NAT gateway so that servers in a VPC can use this EIP to provide services accessible from the Internet.

### Procedure

For details, see the *Elastic IP User Guide*.

You do not need to bind the EIP to any server.

## 2.2.3 Step 2: Create a Public NAT Gateway

### Scenarios

a public NAT gateway to enable your servers to access the Internet or provide services accessible from the Internet.

### Prerequisites

- The VPC and subnet where your public NAT gateway will be deployed are available.
- To allow traffic to pass through the public NAT gateway, a route to the public NAT gateway in the VPC is required. When you create a public NAT gateway, a default route 0.0.0.0/0 to the public NAT gateway is automatically added to the default route table of the VPC. If the default route 0.0.0.0/0 already exists in the default route table of the VPC before you create the public NAT gateway, the default route that points to the public NAT gateway will fail to be added automatically. In this case, perform the following operations after the public NAT gateway is successfully created: Manually add a different route that points to the gateway or create a default route 0.0.0.0/0 pointing to the gateway in the new routing table.

### Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.  
The **Public NAT Gateway** page is displayed.
3. On the displayed page, click **Create Public NAT Gateway**.
4. Configure required parameters. For details, see [Table 2-3](#).

**Table 2-3** Descriptions of public NAT gateway parameters

| Parameter | Description  |
|-----------|--|
| Region    | The region where the public NAT gateway is located |

| Parameter      | Description  |
|----------------|--|
| Name           | The name of the public NAT gateway<br>Enter up to 64 characters. Only digits, letters, underscores (_), hyphens (-), and periods (.) are allowed.  |
| VPC            | The VPC that the public NAT gateway belongs to<br>The selected VPC cannot be changed after you create the public NAT gateway.<br><b>NOTE</b><br>To allow traffic to pass through the public NAT gateway, a route to the public NAT gateway in the VPC is required. When you create a public NAT gateway, a default route 0.0.0.0/0 to the public NAT gateway is automatically added to the default route table of the VPC. If the default route 0.0.0.0/0 already exists in the default route table of the VPC before you create the public NAT gateway, the default route that points to the public NAT gateway will fail to be added automatically. In this case, perform the following operations after the public NAT gateway is successfully created: Manually add a different route that points to the gateway or create a default route 0.0.0.0/0 pointing to the gateway in the new routing table. |
| Subnet         | The subnet that the public NAT gateway belongs to<br>The subnet must have at least one available IP address.<br>The selected subnet cannot be changed after you create the public NAT gateway.<br>The NAT gateway will be deployed in the selected subnet. The NAT gateway works for the entire VPC where it is deployed. To enable communications over the Internet, add SNAT or DNAT rules.  |
| Specifications | The specifications of the public NAT gateway<br>The value can be <b>Extra-large</b> , <b>Large</b> , <b>Medium</b> , or <b>Small</b> . To view more details about specifications, click <b>Learn more</b> on the page.   |
| Description    | Supplementary information about the public NAT gateway<br>Enter up to 255 characters. Angle brackets (<>) are not allowed.   |

5. Click **Create Now**. On the page displayed, confirm the public NAT gateway specifications.
6. Click **Submit**.  
It takes 1 to 6 minutes to create a public NAT gateway.
7. In the list, view the status of the public NAT gateway.

 **NOTE**

After the public NAT gateway is created, check whether a default route (0.0.0.0/0) that points to the public NAT gateway exists in the default route table of the VPC where the public NAT gateway is. If no, add a route pointing to the public NAT gateway to the default route table, alternatively, create a custom route table and add the default route 0.0.0.0/0 pointing to the public NAT gateway to the table. The following describes how to add a route to a custom route table.

## Adding a Default Route Pointing to the Public NAT Gateway

1. Log in to the management console.
2. Under **Network**, select **Virtual Private Cloud**.
3. In the navigation pane on the left, choose **Route Tables**.
4. On the **Route Tables** page, click **Create Route Table** in the upper right corner.  
**VPC:** Select the VPC to which the public NAT gateway belongs.
5. After the custom route table is created, click its name.  
The **Summary** page is displayed.
6. Click **Add Route** and configure parameters as follows:  
**Destination:** Set it to **0.0.0.0/0**.  
**Next Hop Type:** Select **NAT gateway**.  
**Next Hop:** Select the created NAT gateway.
7. Click **OK**.

## 2.2.4 Step 3: Add a DNAT Rule

### Scenarios

After a public NAT gateway is created, add DNAT rules to allow servers in your VPC to provide services accessible from the Internet.

You can configure a DNAT rule for each port on a server. If multiple servers need to provide services accessible from the Internet, create multiple DNAT rules.

### Prerequisites

A public NAT gateway is available.

### Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.  
The **Public NAT Gateway** page is displayed.
3. On the displayed page, click the name of the public NAT gateway on which you need to add a DNAT rule.
4. On the public NAT gateway details page, click the **DNAT Rules** tab.
5. Click **Add DNAT Rule**.

6. Configure required parameters. For details, see [Table 2-4](#).

**Table 2-4** Descriptions of DNAT rule parameters

| Parameter          | Description  |
|--------------------|--|
| Scenario           | Select <b>VPC</b> if your servers in a VPC need to share an EIP to provide services accessible from the Internet.  |
| Port Type          | The port type <ul style="list-style-type: none"><li>• <b>All ports</b>: All requests received by the gateway through all ports over any protocol will be forwarded to the private IP address of your server.</li><li>• <b>Specific port</b>: Only requests received from a specified port over a specified protocol will be forwarded to the specified port on the server.</li></ul> |
| Protocol           | The protocol can be TCP or UDP.<br>This parameter is available if you select <b>Specific port</b> for <b>Port Type</b> . If you select <b>All ports</b> , the value of this parameter is <b>All</b> by default.  |
| EIP                | The EIP of the public NAT gateway<br>You can select an EIP that either has not been bound, has been bound to a DNAT rule of the current public NAT gateway with <b>Port Type</b> set to <b>Specific port</b> , or has been bound to an SNAT rule of the current public NAT gateway.  |
| Outside Port       | The port of the EIP used by the NAT gateway for external communications<br>This parameter is only available if you select <b>Specific port</b> for <b>Port Type</b> .<br>Range: 1 to 65535<br>You can enter a specific port number or a port range, for example, 80 or 80-100.   |
| Private IP Address | The IP address of the server in the NAT gateway's VPC and processes matching packets where requests will be forwarded to<br>Configure the port of <b>Private IP Address</b> if you select <b>Specific port</b> for <b>Port Type</b> .  |
| Inside Port        | The port of the server over which the originating requests will be forwarded<br>This parameter is only available if you select <b>Specific port</b> for <b>Port Type</b> .<br>Range: 1 to 65535<br>You can enter a specific port number or a port range, for example, 80 or 80-100.  |

| Parameter   | Description  |
|-------------|--|
| Description | Provides supplementary information about the DNAT rule. Enter up to 255 characters. Angle brackets (<>) are not allowed. |

7. Click **OK**.

#### NOTICE

After you add a DNAT rule, add rules to the security group associated with the servers to allow inbound or outbound traffic. Otherwise, the DNAT rule does not take effect.

## 2.2.5 Step 4: Test the Connection

### Scenarios

After adding a DNAT rule, you can perform the following steps to verify the connection:

1. Verify that the DNAT rule has been added for the public NAT gateway.
2. Check whether ECS 01 in the private network can be accessed by ECS 02 from the Internet through the NAT gateway (EIP 120.46.131.153 bound to the DNAT rule).

### Prerequisites

A DNAT rule has been added.

### Verifying that the DNAT Rule Has Been Added

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.
3. On the **Public NAT Gateways** page, click the name of the public NAT gateway.
4. In the **DNAT Rules** tab, view details about the DNAT rule and check whether the DNAT rule has been created.

If **Status** of the DNAT rule is **Running**, the DNAT rule has been created.

### Verifying that Servers in a VPC Can Be Accessed from the Internet Through the NAT Gateway

**Step 1** Log in to the management console.

**Step 2** Log in to ECS 02 with an EIP bound.

**Step 3** On ECS 02, ping the EIP (120.46.131.153) to check whether ECS 01 on the private network can be accessed by ECS 02 on the public network through the NAT gateway.

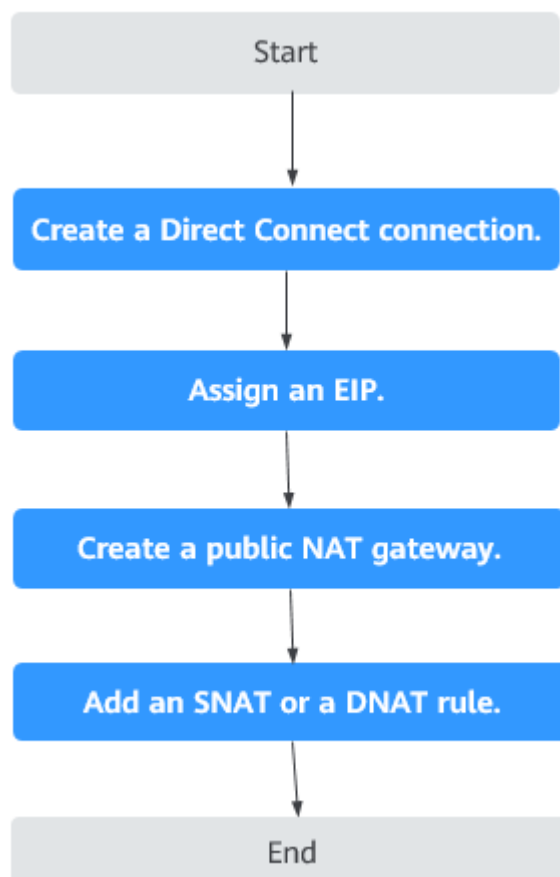
----End

## 2.3 Allowing On-Premises Servers to Communicate with the Internet

### 2.3.1 Overview

You need to first create a Direct Connect or VPN connection to connect your servers in the on-premises data center to the cloud, and then create public NAT gateways and configure SNAT or DNAT rules to allow servers in your data center to access the Internet or to provide services accessible from the Internet. [Figure 2-2](#) shows how servers in an on-premises data center communicate with the Internet.

**Figure 2-2** Servers in an on-premises data center communicating with the Internet



## 2.3.2 Step 1: Connect Your On-premises Data Center to the Cloud with Direct Connect

### Scenarios

Create a Direct Connect connection to link your on-premises data center to a VPC. Then deploy a public NAT gateway in the VPC to allow your on-premises servers to communicate with the Internet.

### Procedure

For details on how to enable Direct Connect, see the *Direct Connect User Guide*.

## 2.3.3 Step 2: Assign an EIP

### Scenarios

Buy an EIP for a public NAT gateway to allow servers that are connected to the cloud using Direct Connect to communicate with the Internet.

### Procedure

For details, see the *Elastic IP User Guide*.

You do not need to bind the EIP to any server.

## 2.3.4 Step 3: Create a Public NAT Gateway

### Scenarios

a public NAT gateway.

### Prerequisites

- You have created the VPC and subnet required for creating a public NAT gateway.
- To allow traffic to pass through the public NAT gateway, a route to the public NAT gateway in the VPC is required. When you create a public NAT gateway, a default route 0.0.0.0/0 to the public NAT gateway is automatically added to the default route table of the VPC. If the default route 0.0.0.0/0 already exists in the default route table of the VPC before you create the public NAT gateway, the default route that points to the public NAT gateway will fail to be added automatically. In this case, perform the following operations after the public NAT gateway is successfully created: Manually add a different route that points to the gateway or create a default route 0.0.0.0/0 pointing to the gateway in the new routing table.

### Procedure

1. Log in to the management console.



2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.

The **Public NAT Gateway** page is displayed.

3. On the displayed page, click **Create Public NAT Gateway**.
4. Configure required parameters. For details, see [Table 2-5](#).

**Table 2-5** Descriptions of public NAT gateway parameters

| Parameter      | Description  |
|----------------|--|
| Region         | The region where the public NAT gateway is located   |
| Name           | The name of the public NAT gateway<br>Enter up to 64 characters. Only digits, letters, underscores (_), and hyphens (-) are allowed.   |
| VPC            | The VPC that the public NAT gateway belongs to<br>The selected VPC cannot be changed after you create the public NAT gateway.<br><b>NOTE</b><br>To allow traffic to pass through the public NAT gateway, a route to the public NAT gateway in the VPC is required. When you create a public NAT gateway, a default route 0.0.0.0/0 to the public NAT gateway is automatically added to the default route table of the VPC. If the default route 0.0.0.0/0 already exists in the default route table of the VPC before you create the public NAT gateway, the default route that points to the public NAT gateway will fail to be added automatically. In this case, perform the following operations after the public NAT gateway is successfully created: Manually add a different route that points to the gateway or create a default route 0.0.0.0/0 pointing to the gateway in the new routing table. |
| Subnet         | The subnet that the public NAT gateway belongs to<br>The subnet must have at least one available IP address.<br>The selected subnet cannot be changed after the public NAT gateway is created.<br>The NAT gateway will be deployed in the selected subnet. The NAT gateway works for the entire VPC where it is deployed. To enable communications over the Internet, add SNAT or DNAT rules.  |
| Specifications | The specifications of the public NAT gateway<br>The value can be <b>Small</b> , <b>Medium</b> , <b>Large</b> , or <b>Extra-large</b> .   |

| Parameter   | Description  |
|-------------|--|
| Description | Supplementary information about the public NAT gateway<br>Enter up to 255 characters. Angle brackets (<>) are not allowed. |

5. Click **Create Now**. On the page displayed, confirm the public NAT gateway specifications.
6. If you do not need to modify the information, click **Submit**.  
It takes 1 to 5 minutes to create a public NAT gateway.
7. In the public NAT gateway list, check the gateway status.

## Adding a Default Route Pointing to the Public NAT Gateway

1. Log in to the management console.
2. Under **Network**, select **Virtual Private Cloud**.
3. In the navigation pane on the left, choose **Route Tables**.
4. On the **Route Tables** page, click **Create Route Table** in the upper right corner.  
**VPC**: Select the VPC to which the public NAT gateway belongs.
5. After the custom route table is created, click its name.  
The **Summary** page is displayed.
6. Click **Add Route** and configure parameters as follows:  
**Destination**: Set it to **0.0.0.0/0**.  
**Next Hop Type**: Select **NAT gateway**.  
**Next Hop**: Select the created NAT gateway.
7. Click **OK**.

### 2.3.5 Step 4: Add an SNAT Rule

#### Scenarios

After a public NAT gateway is created, add SNAT rules for it. With SNAT rules, servers that are connected to a VPC using Direct Connect can access the Internet by sharing an EIP.

Each SNAT rule is configured for only one CIDR block. If servers that are connected to a VPC using Direct Connect are in multiple CIDR blocks, you can create multiple SNAT rules to allow the servers to share EIPs.

#### Prerequisites

A public NAT gateway is available.

## Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.  
The **Public NAT Gateway** page is displayed.
3. On the displayed page, click the name of the public NAT gateway on which you need to add an SNAT rule.
4. On the **SNAT Rules** tab, click **Add SNAT Rule**.
5. Configure required parameters. For details, see [Table 2-6](#).

**Table 2-6** Descriptions of SNAT rule parameters

| Parameter   | Description   |
|-------------|---|
| Scenario    | Select <b>Direct Connect</b> if your on-premises servers need to access the Internet.   |
| CIDR Block  | The CIDR block of the servers in the on-premises data center  |
| EIP         | The EIP used for accessing the Internet<br>You can select an EIP that either has not been bound, has been bound to a DNAT rule of the current public NAT gateway with <b>Port Type</b> set to <b>Specific port</b> , or has been bound to an SNAT rule of the current public NAT gateway. |
| Monitoring  | You can create alarm rules on the Cloud Eye console to monitor your SNAT connections and keep informed of any changes in a timely manner.   |
| Description | Provides supplementary information about the SNAT rule. Enter up to 255 characters. Angle brackets (<>) are not allowed.  |

6. Click **OK**.
7. View details in the SNAT rule list.

If **Status** of the SNAT rule is **Running**, the SNAT rule has been created.

### NOTE

- You can add multiple SNAT rules for a public NAT gateway to suite your service requirements.
- Only one SNAT rule can be added for each VPC subnet.

## 2.3.6 Step 5: Add a DNAT Rule

### Scenarios

After a public NAT gateway is created, add DNAT rules to allow servers in your on-premises data center to provide services accessible from the Internet.

You can configure a DNAT rule for each port on a server. If there are multiple servers, you can create multiple DNAT rules.

### Prerequisites

A public NAT gateway is available.

### Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.  
The **Public NAT Gateway** page is displayed.
3. On the displayed page, click the name of the public NAT gateway on which you need to add a DNAT rule.
4. On the public NAT gateway details page, click the **DNAT Rules** tab.
5. Click **Add DNAT Rule**.
6. Configure required parameters. For details, see [Table 2-7](#).

**Table 2-7** Descriptions of DNAT rule parameters

| Parameter | Description  |
|-----------|--|
| Scenario  | Select <b>Direct Connect</b> if servers in your on-premises data center need to provide services accessible from the Internet.   |
| Port Type | The port type <ul style="list-style-type: none"><li>• <b>All ports</b>: All requests received by the gateway through all ports over any protocol will be forwarded to the private IP address of your server.</li><li>• <b>Specific port</b>: Only requests received from a specified port over a specified protocol will be forwarded to the specified port on the server.</li></ul> |
| Protocol  | The protocol can be TCP or UDP.<br>This parameter is available if you select <b>Specific port</b> for <b>Port Type</b> . If you select <b>All ports</b> , the value of this parameter is <b>All</b> by default.  |

| Parameter          | Description  |
|--------------------|--|
| EIP                | The EIP of the public NAT gateway<br>You can select an EIP that either has not been bound, has been bound to a DNAT rule of the current public NAT gateway with <b>Port Type</b> set to <b>Specific port</b> , or has been bound to an SNAT rule of the current public NAT gateway.  |
| Outside Port       | The port of the EIP used by the NAT gateway for external communications<br>This parameter is only available if you select <b>Specific port</b> for <b>Port Type</b> .<br>Range: 1 to 65535<br>You can enter a specific port number or a port range, for example, 80 or 80-100.   |
| Private IP Address | The IP address of the server that processes matching packets where requests will be forwarded to<br>This IP address is used by local servers that are connected to a VPC through Direct Connect to provide services accessible from the Internet through DNAT. Configure the port of <b>Private IP Address</b> if you select <b>Specific port</b> for <b>Port Type</b> .<br>This IP address is used by the server to provide services accessible from the Internet through DNAT. |
| Inside Port        | The port of the server over which the originating requests will be forwarded<br>This parameter is only available if you select <b>Specific port</b> for <b>Port Type</b> .<br>Range: 1 to 65535<br>You can enter a specific port number or a port range, for example, 80 or 80-100.  |
| Description        | Provides supplementary information about the DNAT rule. Enter up to 255 characters. Angle brackets (<>) are not allowed.   |

7. Click **OK**.

#### NOTICE

After you add a DNAT rule, add rules to the security group associated with the servers to allow inbound or outbound traffic. Otherwise, the DNAT rule does not take effect.

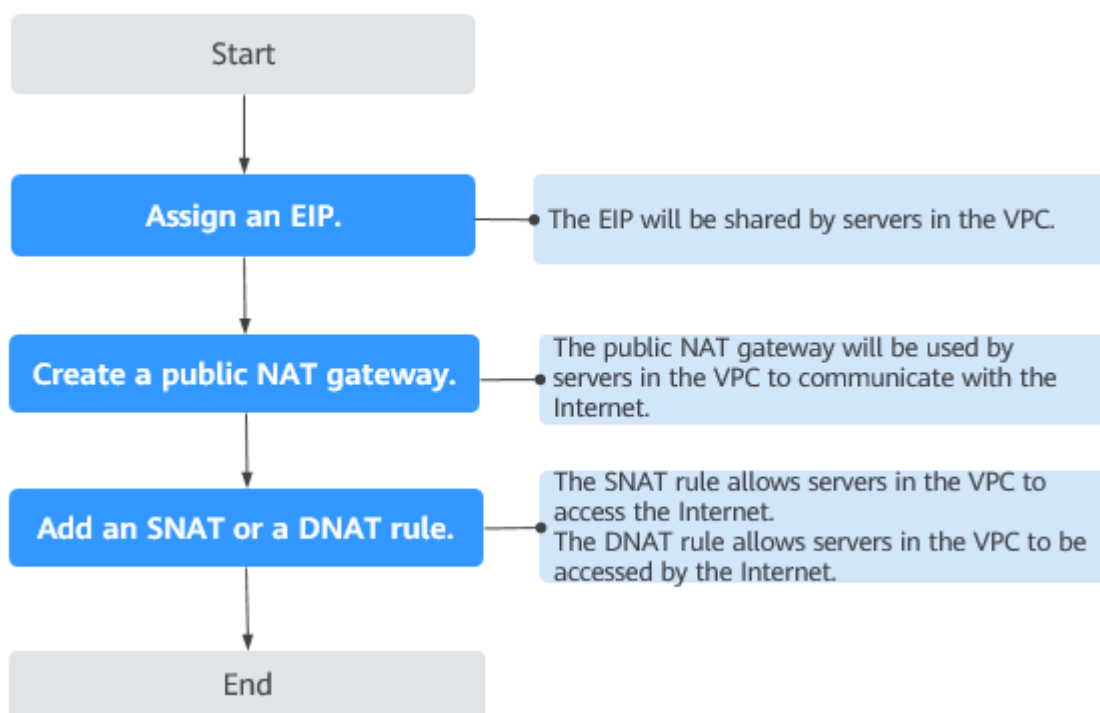
# 3 Public NAT Gateways

## 3.1 Public NAT Gateway Overview

A public NAT gateway enables cloud and on-premises servers in a private subnet to access the Internet or provide services accessible from the Internet. Cloud servers are ECSs and BMSs in a VPC. On-premises servers are servers in on-premises data centers that connect to a VPC through Direct Connect or VPN. A public NAT gateway supports up to 20 Gbit/s of bandwidth.

The process of using a public NAT gateway is as follows.

**Figure 3-1** Process of using a public NAT gateway



 NOTE

An SNAT rule and a DNAT rule cannot share the same EIP. If you need to create an SNAT rule and a DNAT rule, assign two EIPs.

## 3.2 Managing Public NAT Gateways

### 3.2.1 Creating a Public NAT Gateway

#### Scenarios

a public NAT gateway to enable your servers to access the Internet or provide services accessible from the Internet.

#### Constraints and Limitations

- Rules on one public NAT gateway can use the same EIP, but rules on different NAT gateways must use different EIPs.
- Each VPC can have only one NAT gateway.
- SNAT and DNAT rules cannot use the same EIP.
- If both an EIP and a public NAT gateway are configured for a server, data will be forwarded through the EIP.

#### Prerequisites

- The VPC and subnet where your public NAT gateway will be deployed are available.
- To allow traffic to pass through the public NAT gateway, a route to the public NAT gateway in the VPC is required. When you create a public NAT gateway, a default route 0.0.0.0/0 to the public NAT gateway is automatically added to the default route table of the VPC. If the default route 0.0.0.0/0 already exists in the default route table of the VPC before you create the public NAT gateway, the default route that points to the public NAT gateway will fail to be added automatically. In this case, perform the following operations after the public NAT gateway is successfully created: Manually add a different route that points to the gateway or create a default route 0.0.0.0/0 pointing to the gateway in the new routing table.

#### Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.  
The **Public NAT Gateway** page is displayed.
3. On the displayed page, click **Create Public NAT Gateway**.
4. Configure required parameters. For details, see [Table 3-1](#).

**Table 3-1** Descriptions of public NAT gateway parameters

| Parameter      | Description  |
|----------------|--|
| Region         | The region where the public NAT gateway is located   |
| Name           | The name of the public NAT gateway<br>Enter up to 64 characters. Only digits, letters, underscores (_), hyphens (-), and periods (.) are allowed.  |
| VPC            | The VPC that the public NAT gateway belongs to<br>The selected VPC cannot be changed after you create the public NAT gateway.<br><b>NOTE</b><br>To allow traffic to pass through the public NAT gateway, a route to the public NAT gateway in the VPC is required. When you create a public NAT gateway, a default route 0.0.0.0/0 to the public NAT gateway is automatically added to the default route table of the VPC. If the default route 0.0.0.0/0 already exists in the default route table of the VPC before you create the public NAT gateway, the default route that points to the public NAT gateway will fail to be added automatically. In this case, perform the following operations after the public NAT gateway is successfully created: Manually add a different route that points to the gateway or create a default route 0.0.0.0/0 pointing to the gateway in the new routing table. |
| Subnet         | The subnet that the public NAT gateway belongs to<br>The subnet must have at least one available IP address.<br>The selected subnet cannot be changed after you create the public NAT gateway.<br>The NAT gateway will be deployed in the selected subnet. The NAT gateway works for the entire VPC where it is deployed. To enable communications over the Internet, add SNAT or DNAT rules.  |
| Specifications | The specifications of the public NAT gateway<br>The value can be <b>Extra-large</b> , <b>Large</b> , <b>Medium</b> , or <b>Small</b> . To view more details about specifications, click <b>Learn more</b> on the page.   |
| Description    | Supplementary information about the public NAT gateway<br>Enter up to 255 characters. Angle brackets (<>) are not allowed.   |

5. Click **Create Now**. On the page displayed, confirm the public NAT gateway specifications.
6. Click **Submit**.  
It takes 1 to 6 minutes to create a public NAT gateway.
7. In the list, view the status of the public NAT gateway.



## Adding a Default Route Pointing to the Public NAT Gateway

1. Log in to the management console.
2. Under **Network**, select **Virtual Private Cloud**.
3. In the navigation pane on the left, choose **Route Tables**.
4. On the **Route Tables** page, click **Create Route Table** in the upper right corner.  
**VPC**: Select the VPC to which the public NAT gateway belongs.
5. After the custom route table is created, click its name.  
The **Summary** page is displayed.
6. Click **Add Route** and configure parameters as follows:  
**Destination**: Set it to **0.0.0.0/0**.  
**Next Hop Type**: Select **NAT gateway**.  
**Next Hop**: Select the created NAT gateway.
7. Click **OK**.

### NOTE

After the public NAT gateway is created, check whether a default route (0.0.0.0/0) that points to the public NAT gateway exists in the default route table of the VPC where the public NAT gateway is. If no, add a route pointing to the public NAT gateway to the default route table, alternatively, create a custom route table and add the default route 0.0.0.0/0 pointing to the public NAT gateway to the table. The following describes how to add a route to a custom route table.

## 3.2.2 Viewing a Public NAT Gateway

### Scenarios

View information about a public NAT gateway.

### Prerequisites

A public NAT gateway is available.

### Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.  
The **Public NAT Gateway** page is displayed.
3. Click the name of the public NAT gateway.
4. View information about the public NAT gateway.

## 3.2.3 Modifying a Public NAT Gateway

### Scenarios

Modify the name, specifications, or description of a public NAT gateway.

Using a public NAT gateway of more robust specifications does not affect services, but if you switch to a public NAT gateway of less robust specifications, ensure that its capacity can still be enough to meet your service requirements.

## Prerequisites

A public NAT gateway is available.

## Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.  
The **Public NAT Gateway** page is displayed.
3. Locate the row that contains the public NAT gateway you want to modify and click **Modify** in the **Operation** column.
4. Modify the name, specifications, or description of the public NAT gateway.

## 3.2.4 Deleting a Public NAT Gateway

### Scenarios

Delete public NAT gateways that are no longer required to release resources.

### Prerequisites

- All SNAT and DNAT rules created on the public NAT gateway have been deleted. For details about how to delete SNAT and DNAT rules, see [Deleting an SNAT Rule](#) and [Deleting a DNAT Rule](#).

### Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.  
The **Public NAT Gateway** page is displayed.
3. On the displayed page, locate the public NAT gateway that you want to delete and click **Delete** in the **Operation** column.
4. In the displayed dialog box, enter **DELETE**.
5. Click **OK**.

## 3.3 Managing SNAT Rules

## 3.3.1 Adding an SNAT Rule

### Scenarios

After a public NAT gateway is created, add an SNAT rule, so that servers in a VPC subnet or servers that are connected to a VPC through Direct Connect can access the Internet by sharing an EIP.

One SNAT rule takes effect for only one subnet. If there are multiple subnets in a VPC, create multiple SNAT rules to allow servers in them to share EIPs.

### Constraints and Limitations

- Only one SNAT rule can be added for each VPC subnet.
- When you add an SNAT rule in the VPC scenario, the custom CIDR block must be a subset of the NAT gateway's VPC subnets.
- If an SNAT rule is used in the Direct Connect scenario, the custom CIDR block must be a CIDR block of a Direct Connect connection and cannot overlap with the NAT gateway's VPC subnets.
- There is no limit on the number of SNAT rules that can be added on a public NAT gateway.

### Prerequisites

A public NAT gateway is available.

### Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.  
The **Public NAT Gateway** page is displayed.
3. On the displayed page, click the name of the public NAT gateway on which you need to add an SNAT rule.
4. On the **SNAT Rules** tab, click **Add SNAT Rule**.
5. Configure required parameters. For details, see [Table 3-2](#).

**Table 3-2** Descriptions of SNAT rule parameters

| Parameter | Description  |
|-----------|--|
| Scenario  | The scenarios where the SNAT rule is used<br>Select <b>VPC</b> if your servers in a VPC need to access the Internet.<br>Select <b>Direct Connect</b> if servers in your on-premises data center need to access the Internet. |

| Parameter              | Description   |
|------------------------|---|
| CIDR Block             | In a VPC scenario, specify a VPC subnet to enable servers in that subnet to access the Internet using the SNAT rule.<br><br>In a Direct Connect scenario, specify a CIDR block of your data center to enable your servers to access the Internet using the SNAT rule.                     |
| Public IP Address Type | The EIP used for accessing the Internet<br>You can select an EIP that either has not been bound, has been bound to a DNAT rule of the current public NAT gateway with <b>Port Type</b> set to <b>Specific port</b> , or has been bound to an SNAT rule of the current public NAT gateway. |
| Monitoring             | You can create alarm rules on the Cloud Eye console to monitor your SNAT connections and keep informed of any changes in a timely manner.   |
| Description            | Provides supplementary information about the SNAT rule. Enter up to 255 characters. Angle brackets (<>) are not allowed.  |

- Click **OK**.

 **NOTE**

- You can add multiple SNAT rules for a public NAT gateway to suite your service requirements.
- Only one SNAT rule can be added for each VPC subnet.

## 3.3.2 Viewing an SNAT Rule

### Scenarios

View details about an SNAT rule.

### Prerequisites

An SNAT rule has been added.

### Procedure

- Log in to the management console.
- Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.  
The **Public NAT Gateway** page is displayed.
- Click the name of the public NAT gateway.
- In the SNAT rule list, view details about the SNAT rule.

## 3.3.3 Deleting an SNAT Rule

### Scenarios

Delete an SNAT rule that you no longer need.

### Prerequisites

An SNAT rule has been added.

### Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.  
The **Public NAT Gateway** page is displayed.
3. Click the name of the public NAT gateway.
4. In the SNAT rule list, locate the row that contains the SNAT rule you want to delete and click **Delete** in the **Operation** column.
5. Enter **DELETE** in the displayed dialog box and click **OK**.

## 3.4 Managing DNAT Rules

### 3.4.1 Adding a DNAT Rule

#### Scenarios

After a public NAT gateway is created, add DNAT rules to allow servers in your VPC to provide services accessible from the Internet.

Only one DNAT rule can be configured for each port on a server. One port can be mapped to only one EIP. If multiple servers need to provide services accessible from the Internet, create multiple DNAT rules.

#### Restrictions and Limitations

- DNAT rules cannot map virtual IP addresses to EIPs.
- Only one DNAT rule can be configured for each port on a server. One port can be mapped to only one EIP.
- A maximum of 200 DNAT rules can be added on a public NAT gateway.

#### Prerequisites

A public NAT gateway is available.

#### Procedure

1. Log in to the management console.

2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.  
The **Public NAT Gateway** page is displayed.
3. On the displayed page, click the name of the public NAT gateway on which you need to add a DNAT rule.
4. On the public NAT gateway details page, click the **DNAT Rules** tab.
5. Click **Add DNAT Rule**.
6. Configure required parameters. For details, see [Table 3-3](#).

**Table 3-3** Descriptions of DNAT rule parameters

| Parameter              | Description   |
|------------------------|---|
| Scenario               | Select <b>VPC</b> if your servers in a VPC will use the DNAT rule to share the same EIP to provide services accessible from the Internet.<br><br><b>Direct Connect:</b> Select this scenario if your on-premises servers will use the DNAT rule to provide services accessible from the Internet.   |
| Port Type              | The port type <ul style="list-style-type: none"> <li>• <b>All ports:</b> All requests received by the gateway through all ports over any protocol will be forwarded to the private IP address of your server.</li> <li>• <b>Specific port:</b> Only requests received from a specified port over a specified protocol will be forwarded to the specified port on the server.</li> </ul> |
| Protocol               | The protocol can be TCP or UDP.<br>This parameter is available if you select <b>Specific port</b> for <b>Port Type</b> . If you select <b>All ports</b> , the value of this parameter is <b>All</b> by default.   |
| Public IP Address Type | The EIP that will be used by the server to provide services accessible from the Internet<br>You can select an EIP that either has not been bound, has been bound to a DNAT rule of the current public NAT gateway with <b>Port Type</b> set to <b>Specific port</b> , or has been bound to an SNAT rule of the current public NAT gateway.  |
| Outside Port           | The port of the EIP used by the NAT gateway for external communication<br>This parameter is only available if you select <b>Specific port</b> for <b>Port Type</b> . Range: 1 to 65535<br>You can enter a specific port number or a port range, for example, 80 or 80-100.  |

| Parameter          | Description  |
|--------------------|--|
| Instance Type      | The type of the instance that will be providing services accessible from the Internet. Possible values are: <ul style="list-style-type: none"><li>• <b>Server</b></li><li>• <b>Virtual IP address</b></li><li>• <b>Custom</b></li></ul>  |
| NIC                | The NIC of the server. This parameter is available if you set <b>Instance Type</b> to <b>Server</b> .  |
| Private IP Address | <ul style="list-style-type: none"><li>• In a VPC scenario, set this parameter to the private IP address of a server in the NAT gateway's VPC. The server will provide services accessible from the Internet through DNAT.</li><li>• In a Direct Connect scenario, set this parameter to IP address of the server in your on-premises data center or your private IP address. This IP address is used by on-premises servers that are connected to a VPC through Direct Connect to provide services accessible from the Internet through DNAT.</li><li>• Configure the port of <b>Private IP Address</b> if you select <b>Specific port</b> for <b>Port Type</b>.</li></ul> |
| Inside Port        | The port of the server over which the originating requests will be forwarded<br>This parameter is only available if you select <b>Specific port</b> for <b>Port Type</b> .<br>Range: 1 to 65535<br>You can enter a specific port number or a port range, for example, 80 or 80-100.  |
| Description        | Provides supplementary information about the DNAT rule. Enter up to 255 characters. Angle brackets (<>) are not allowed.   |

7. Click **OK**.

Once the rule is created, its status changes to **Running**.

**NOTICE**

After you add a DNAT rule, add rules to the security group associated with the servers to allow inbound or outbound traffic. Otherwise, the DNAT rule does not take effect.

## 3.4.2 Viewing a DNAT Rule

### Scenarios

View details about a DNAT rule.

### Prerequisites

A DNAT rule has been added.

### Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.  
The **Public NAT Gateway** page is displayed.
3. Click the name of the public NAT gateway.
4. On the public NAT gateway details page, click the **DNAT Rules** tab.
5. In the DNAT rule list, view details about the DNAT rule.

## 3.4.3 Modifying a DNAT Rule

### Scenarios

Modify a DNAT rule.

### Prerequisites

A DNAT rule has been added.

### Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.  
The **Public NAT Gateway** page is displayed.
3. Click the name of the public NAT gateway.
4. On the public NAT gateway details page, click the **DNAT Rules** tab.
5. In the DNAT rule list, locate the row that contains the DNAT rule you want to modify and click **Modify** in the **Operation** column.
6. In the displayed dialog box, modify parameters as needed.
7. Click **OK**.

## 3.4.4 Deleting a DNAT Rule

### Scenarios

Delete a DNAT rule that you no longer need.



## Prerequisites

A DNAT rule has been added.

## Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.  
The **Public NAT Gateway** page is displayed.
3. Click the name of the public NAT gateway.
4. On the public NAT gateway details page, click the **DNAT Rules** tab.
5. In the DNAT rule list, locate the row that contains the DNAT rule you want to delete and click **Delete** in the **Operation** column.
6. Enter **DELETE** in the displayed dialog box and click **OK**.

## 3.4.5 Deleting DNAT Rules in Batches

### Scenarios

Delete DNAT rules that you no longer need.

### Prerequisites

DNAT rules have been added.

### Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.  
The **Public NAT Gateway** page is displayed.
3. Click the name of the public NAT gateway.
4. On the public NAT gateway details page, click the **DNAT Rules** tab.
5. In the DNAT rule list, select DNAT rules that you no longer need and click **Delete DNAT Rule**.
6. In the displayed dialog box, click **Yes**.

# 4 Private NAT Gateways

---

## 4.1 Private NAT Gateway Overview

### Private NAT Gateways

Private NAT gateways provide private address translation services for ECSs and BMSs in a VPC. You can configure SNAT and DNAT rules to translate the source and destination IP addresses into transit IP addresses, so that servers in the VPC can communicate with other VPCs or on-premises data centers.

Specifically:

- SNAT enables servers across AZs in a VPC to share a transit IP address to access on-premises data centers or other VPCs.
- DNAT enables servers across AZs in a VPC to share a transit IP address to provide services accessible from on-premises data centers or other VPCs.

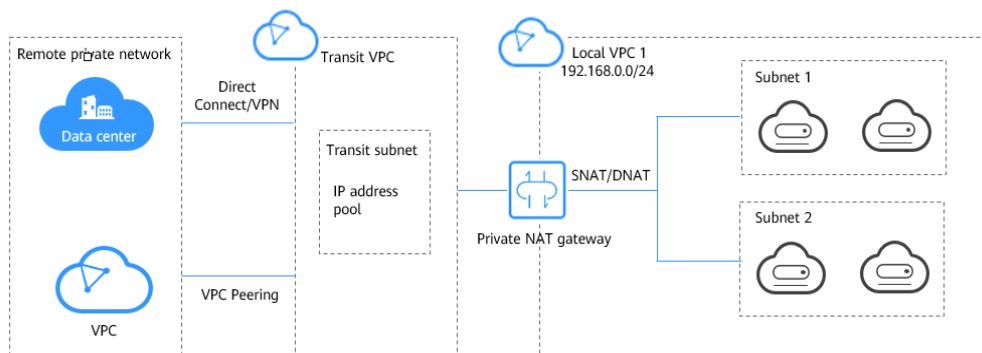
### Transit Subnet

A transit subnet functions as a transit network. You can configure a transit IP address for the transit subnet so that servers in a local VPC can share the transit IP address to access on-premises data centers or other VPCs.

### Transit VPC

The transit VPC is the VPC that the transit subnet is a part of.

**Figure 4-1** Private NAT gateway



## Differences Between Public and Private NAT Gateways

Public NAT gateways use SNAT rules to map private IP addresses to EIPs, so that servers in a VPC can share an EIP to access the Internet. DNAT rules enable the servers to share an EIP to provide services accessible from the Internet.

Private NAT gateways use SNAT rules to map private IP addresses to transit IP addresses, so that servers in a VPC can access on-premises data centers or other VPCs. DNAT rules enable the servers to share the transit IP address to provide services accessible from the private network.

**Table 4-1** describes the differences between public and private NAT gateways.

**Table 4-1** Differences between public and private NAT gateways

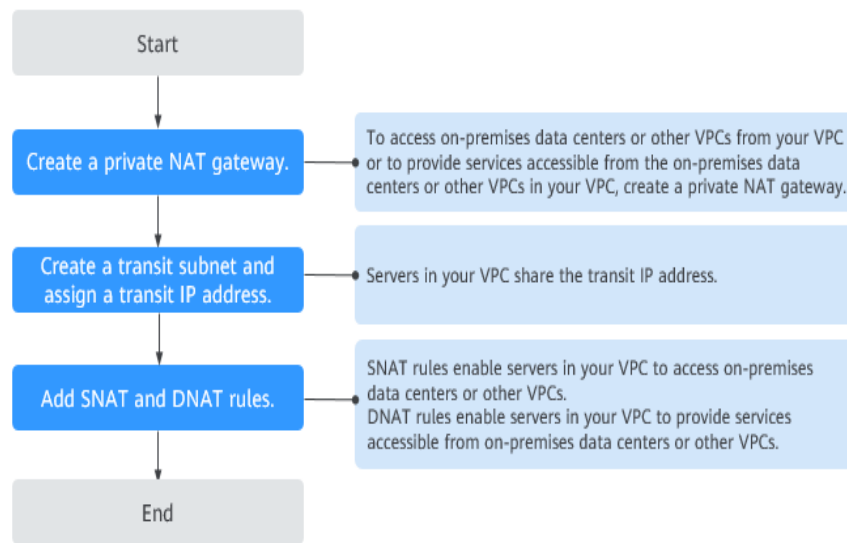
| Item                 | Public NAT Gateway  | Private NAT Gateway   |
|----------------------|---|---|
| Function             | Connects a private network to the Internet                      | Connects private networks   |
| SNAT                 | Enables access to the Internet                                  | Enables access to on-premises data centers or other VPCs  |
| DNAT                 | Allows servers to provide services accessible from the Internet | Allows servers to provide services accessible from on-premises data centers or other VPCs in private networks |
| Communications media | EIP   | Transit IP address  |

## 4.2 Creating a Private NAT Gateway

### 4.2.1 Overview

This section describes how to deploy a private NAT gateway.

**Figure 4-2** Process for deploying a private NAT gateway



If you want to use a private NAT gateway to connect your VPC to on-premises data centers or other VPCs, refer to [Accessing On-premises Data Centers or Other VPCs](#).

## 4.2.2 Creating a Private NAT Gateway

### Scenarios

You can create a private NAT gateway to enable servers in your VPC to access or provide services accessible from on-premises data centers and other VPCs.

### Constraints and Limitations

- Manually add routes in a VPC to connect it to a remote private network through a VPC peering connection, Direct Connect, or VPN connection.
- SNAT and DNAT rules cannot share a transit IP address.
- The total number of DNAT and SNAT rules that can be added on a private NAT gateway varies with the private NAT gateway specifications.
  - Small: 20 or less
  - Medium: 50 or less
  - Large: 200 or less
  - Extra-large: 500 or less

#### CAUTION

When you create a private NAT gateway, you must specify its VPC, subnet, and specifications.

## Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.  
The NAT gateway console is displayed.
3. In the navigation pane on the left, choose **NAT Gateway > Private NAT Gateways**.
4. On the **Private NAT Gateways** page, click **Create Private NAT Gateway**.
5. Configure required parameters. For details, see [Table 4-2](#).

**Table 4-2** Descriptions of private NAT gateway parameters

| Parameter      | Description  |
|----------------|--|
| Region         | The region where the private NAT gateway is located  |
| Name           | The name of the private NAT gateway<br>Enter up to 64 characters. Only digits, letters, underscores (_), hyphens (-), and periods (.) are allowed.   |
| VPC            | The VPC that the private NAT gateway belongs to<br>The selected VPC cannot be changed after the private NAT gateway is created.  |
| Subnet         | The subnet that the private NAT gateway belongs to<br>The subnet must have at least one available IP address.<br>The selected subnet cannot be changed after the private NAT gateway is created.                           |
| Specifications | The specifications of the private NAT gateway<br>The value can be <b>Extra-large</b> , <b>Large</b> , <b>Medium</b> , or <b>Small</b> . For details about specifications, see <a href="#">NAT Gateway Specifications</a> . |
| Description    | Supplementary information about the private NAT gateway<br>Enter up to 255 characters. Angle brackets (<>) are not allowed.  |

6. Click **Create Now**.

## Helpful Links

[Managing Private NAT Gateways](#)

## 4.2.3 Assigning a Transit IP Address

### Scenarios

After a private NAT gateway is created, create a transit subnet and assign a transit IP address, so that servers in your VPC can share the transit IP address to communicate with on-premises data centers or other VPCs.

### Prerequisites

- There are transit VPCs available.

### Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.  
The NAT gateway console is displayed.
3. In the navigation pane on the left, choose **NAT Gateway > Private NAT Gateways**.
4. Click **OK**.

### Helpful Links

[Managing Transit Subnets](#)

## 4.2.4 Adding an SNAT Rule

### Scenarios

After the private NAT gateway is created, add an SNAT rule so that some or all servers in a VPC subnet can share a transit IP address to access on-premises data centers or other VPCs.

### Constraints and Limitations

- Only one SNAT rule can be added for each VPC subnet.

### Prerequisites

- A private NAT gateway is available.
- Transit IP addresses are available.

### Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.  
The NAT gateway console is displayed.
3. In the navigation pane on the left, choose **NAT Gateway > Private NAT Gateways**.

4. On the **Private NAT Gateways** page, click the name of the private NAT gateway on which you need to add an SNAT rule.
5. On the **SNAT Rules** tab, click **Add SNAT Rule**.
6. Configure required parameters. For details, see [Table 4-3](#).

**Table 4-3** Parameter descriptions of an SNAT rule

| Parameter          | Description   |
|--------------------|---|
| Subnet             | The subnet type of the SNAT rule. Select <b>Existing</b> or <b>Custom</b> .<br>Select a subnet where IP address translation is required in the service VPC. |
| Monitoring         | You can create alarm rules to watch the number of SNAT connections.   |
| Transit IP Address | Select the created transit IP address.  |
| Description        | Provides supplementary information about the SNAT rule. Enter up to 255 characters. Angle brackets (<>) are not allowed.                                    |

7. Click **OK**.

 **NOTE**

You can add multiple SNAT rules for a private NAT gateway to suite your service requirements.

## Helpful Links

[Managing SNAT Rules](#)

## 4.2.5 Adding a DNAT Rule

### Scenarios

After a private NAT gateway is created, you can add DNAT rules to allow servers in your VPC to provide services accessible from on-premises servers or other VPCs.

A DNAT rule needs to be configured for each port on a server that needs to be made accessible. If multiple ports on a server or multiple servers need to provide services accessible from on-premises servers or other VPCs, multiple DNAT rules need to be configured.

### Constraints and Limitations

- A DNAT rule with **Port Type** set to **All ports** cannot share a transit IP address with a DNAT rule with **Port Type** set to **Specific port**.

### Prerequisites

- A private NAT gateway is available.

- Transit IP addresses and transit subnets are available.

## Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.  
The NAT gateway console is displayed.
3. In the navigation pane on the left, choose **NAT Gateway > Private NAT Gateways**.
4. On the **Private NAT Gateways** page, click the name of the private NAT gateway on which you need to add a DNAT rule.
5. On the private NAT gateway details page, click the **DNAT Rules** tab.
6. Click **Add DNAT Rule**.

### NOTICE

After you add a DNAT rule, add rules to the security group associated with the servers to allow inbound or outbound traffic. Otherwise, the DNAT rule does not take effect.

7. Configure required parameters. For details, see [Table 4-4](#).

**Table 4-4** Descriptions of DNAT rule parameters

| Parameter | Description  |
|-----------|--|
| Port Type | <p>The port type</p> <p>The type can be:</p> <ul style="list-style-type: none"> <li>• <b>Specific port:</b> The private NAT gateway only forwards requests to your servers from the outside port and to the inside port configured here, and only if they use the right protocol.</li> <li>• <b>All ports:</b> All requests received by the gateway through all ports over any protocol will be forwarded to the private IP address of your server.</li> </ul> |
| Protocol  | <p>The protocol can be TCP or UDP</p> <p>If you select <b>All ports</b>, the value of this parameter is <b>All</b> by default.</p> <p>This parameter is only available if you select <b>Specific port</b> for <b>Port Type</b>.</p>  |



| Parameter               | Description   |
|-------------------------|---|
| Instance Type           | The type of instance that will provide services accessible from on-premises data centers or other VPCs<br>Possible types are: <ul style="list-style-type: none"> <li>• <b>Server</b></li> <li>• <b>Virtual IP address</b></li> <li>• <b>Load balancer</b></li> <li>• <b>Custom</b></li> </ul>   |
| NIC                     | The NIC of the server<br>This parameter is only available if you set <b>Instance Type</b> to <b>Server</b> .  |
| IP Address              | The IP address of the server that will provide services accessible from on-premises data centers or other VPCs. This parameter is only available if you set <b>Instance Type</b> to <b>Custom</b> .   |
| Internal Port           | The port of the instance<br>Range: 1 to 65535<br>This parameter is only available if you select <b>Specific port</b> for <b>Port Type</b> .   |
| <b>Transit Network</b>  |   |
| Transit IP Address      | The transit IP address used to access on-premises data centers or other VPCs<br>You can select a transit IP address that is not bound to any resource, has been bound to a DNAT rule for the current private NAT gateway where <b>Port Type</b> is set to <b>Specific port</b> , or has been bound to a SNAT rule of the current private NAT gateway. |
| Transit IP Address Port | The port of the transit IP address Supported range: 1 to 65535<br>This parameter is only available if you select <b>Specific port</b> for <b>Port Type</b> .  |
| Description             | Provides supplementary information about the DNAT rule. Enter up to 255 characters. Angle brackets (<>) are not allowed.  |

- Click **OK**.  
Once the rule is created, its status changes to **Running**.

## Helpful Links

[Managing DNAT Rules](#)

## 4.3 Managing Private NAT Gateways

### 4.3.1 Viewing a Private NAT Gateway

#### Scenarios

View information about a private NAT gateway.

#### Prerequisites

A private NAT gateway is available.

#### Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.  
The NAT gateway console is displayed.
3. In the navigation pane on the left, choose **NAT Gateway > Private NAT Gateways**.
4. On the **Private NAT Gateways** page, click the name of the private NAT gateway.
5. On the displayed page, view information about the private NAT gateway.

### 4.3.2 Modifying a Private NAT Gateway

#### Scenarios

Modify the name, specifications, or description of a private NAT gateway.

#### Prerequisites

A private NAT gateway is available.

#### Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.  
The NAT gateway console is displayed.
3. In the navigation pane on the left, choose **NAT Gateway > Private NAT Gateways**.
4. On the **Private NAT Gateways** page, locate the row that contains the private NAT gateway you want to modify and click **Modify** in the **Operation** column.
5. Modify the name, specifications, or description of the private NAT gateway.

6. Click **Next**.
7. Confirm the modification and click **Submit**.

### 4.3.3 Deleting a Private NAT Gateway

#### Scenarios

Delete private NAT gateways that are no longer required to release resources.

#### Prerequisites

All SNAT and DNAT rules created on the private NAT gateway have been deleted. For details about how to delete SNAT and DNAT rules, see [Deleting an SNAT Rule](#) and [Deleting a DNAT Rule](#).

#### Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.  
The NAT gateway console is displayed.
3. In the navigation pane on the left, choose **NAT Gateway > Private NAT Gateways**.
4. On the **Private NAT Gateways** page, locate the private NAT gateway that you want to delete and click **Delete** in the **Operation** column.
5. In the displayed dialog box, enter **DELETE**.
6. Click **OK**.

## 4.4 Managing SNAT Rules

### 4.4.1 Viewing an SNAT Rule

#### Scenarios

View details about an SNAT rule.

#### Prerequisites

An SNAT rule has been added.

#### Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.  
The NAT gateway console is displayed.
3. In the navigation pane on the left, choose **NAT Gateway > Private NAT Gateways**.

4. On the **Private NAT Gateways** page, click the name of the private NAT gateway.
5. In the SNAT rule list, view details about the SNAT rule.

## 4.4.2 Modifying an SNAT Rule

### Scenarios

Modify an SNAT rule.

### Prerequisites

An SNAT rule has been added.

### Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.  
The NAT gateway console is displayed.
3. In the navigation pane on the left, choose **NAT Gateway > Private NAT Gateways**.
4. On the **Private NAT Gateways** page, click the name of the private NAT gateway.
5. On the **SNAT Rules** tab, locate the row that contains the SNAT rule you want to modify.
6. Click **Modify** in the **Operation** column.
7. In the displayed dialog box, modify parameters as needed.
8. Click **OK**.

## 4.4.3 Deleting an SNAT Rule

### Scenarios

Delete SNAT rules that you no longer need.

### Prerequisites

An SNAT rule has been added.

### Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.  
The NAT gateway console is displayed.
3. In the navigation pane on the left, choose **NAT Gateway > Private NAT Gateways**.

4. On the **Private NAT Gateways** page, click the name of the private NAT gateway.
5. In the SNAT rule list, locate the row that contains the SNAT rule you want to delete and click **Delete** in the **Operation** column.
6. In the displayed dialog box, click **Yes**.

## 4.5 Managing DNAT Rules

### 4.5.1 Viewing a DNAT Rule

#### Scenarios

View details about a DNAT rule.

#### Prerequisites

A DNAT rule has been added.

#### Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.  
The NAT gateway console is displayed.
3. In the navigation pane on the left, choose **NAT Gateway > Private NAT Gateways**.
4. On the **Private NAT Gateways** page, click the name of the private NAT gateway.
5. On the private NAT gateway details page, click the **DNAT Rules** tab.
6. In the DNAT rule list, view details about the DNAT rule.

### 4.5.2 Modifying a DNAT Rule

#### Scenarios

Modify a DNAT rule.

#### Prerequisites

A DNAT rule has been added.

#### Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.  
The NAT gateway console is displayed.

3. In the navigation pane on the left, choose **NAT Gateway > Private NAT Gateways**.
4. On the **Private NAT Gateways** page, click the name of the private NAT gateway.
5. On the private NAT gateway details page, click the **DNAT Rules** tab.
6. In the DNAT rule list, locate the row that contains the DNAT rule you want to modify and click **Modify** in the **Operation** column.
7. In the displayed dialog box, modify parameters as needed.
8. Click **OK**.

### 4.5.3 Deleting a DNAT Rule

#### Scenarios

Delete a DNAT rule that you no longer need.

#### Prerequisites

A DNAT rule has been added.

#### Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.  
The NAT gateway console is displayed.
3. In the navigation pane on the left, choose **NAT Gateway > Private NAT Gateways**.
4. On the **Private NAT Gateways** page, click the name of the private NAT gateway.
5. On the private NAT gateway details page, click the **DNAT Rules** tab.
6. In the DNAT rule list, locate the row that contains the DNAT rule you want to delete and click **Delete** in the **Operation** column.
7. In the displayed dialog box, click **Yes**.

## 4.6 Managing Transit Subnets

### 4.6.1 Creating a Transit Subnet

#### Scenarios

Create a transit subnet for servers in a VPC to use a transit IP address to access or provide services accessible from on-premises data centers or other VPCs.

## Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.  
The NAT gateway console is displayed.
3. In the navigation pane on the left, choose **NAT Gateway > Private NAT Gateways**.
4. Click the **Transit Subnets** tab and then **Create Transit Subnet**.
5. Configure required parameters. For details, see [Table 4-5](#).

**Table 4-5** Descriptions of transit subnet parameters

| Parameter   | Description  |
|-------------|--|
| Name        | The transit subnet name. Enter up to 64 characters including only digits, letters, underscores (_), and hyphens (-).   |
| VPC         | The VPC that the transit subnet is part of   |
| Subnet      | The subnet that the transit IP address is part of  |
| Description | Supplementary information about the transit subnet<br>Enter up to 255 characters. Angle brackets (<>) are not allowed. |

## 4.6.2 Viewing a Transit Subnet

### Scenarios

View details about a transit subnet.

### Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.  
The NAT gateway console is displayed.
3. In the navigation pane on the left, choose **NAT Gateway > Private NAT Gateways**.
4. Click the **Transit Subnets** tab.
5. In the transit subnet list, click the name of the transit subnet to view its details.

## 4.6.3 Modifying a Transit Subnet

### Scenarios

Modify the total number of IP addresses, name, and description of a transit subnet.

### Changing the Total Number of IP Addresses

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.  
The NAT gateway console is displayed.
3. In the navigation pane on the left, choose **NAT Gateway > Private NAT Gateways**.
4. On the **Transit Subnets** tab page, locate the transit subnet you want to modify, and choose **More > Apply to Change the Number of IP Addresses** in the **Operation** column.
5. Modify the number of IP addresses and click **OK**.

### Modifying the Name or Description of a Transit Subnet

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.  
The NAT gateway console is displayed.
3. In the navigation pane on the left, choose **NAT Gateway > Private NAT Gateways**.
4. On the **Transit Subnets** tab page, locate the transit subnet you want to modify, and click **Modify** in the **Operation** column.
5. Modify the transit subnet name or description and click **OK**.

## 4.6.4 Deleting a Transit Subnet

### Scenarios

Delete a transit subnet that you no longer need.

After the transit subnet is deleted, servers in the VPC where the transit subnet is deployed can no longer communicate with other private networks through the private NAT gateway.

### Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.  
The NAT gateway console is displayed.



3. In the navigation pane on the left, choose **NAT Gateway > Private NAT Gateways**.
4. On the **Transit Subnets** tab page, locate the transit subnet you want to delete, and click **Delete** in the **Operation** column.
5. Click **Yes**.

## 4.7 Managing Transit IP Addresses

### 4.7.1 Assigning a Transit IP Address

#### Scenarios

Servers in a VPC all use the same transit IP address to access or provide services accessible from on-premises data centers or other VPCs.

#### Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.  
The NAT gateway console is displayed.
3. In the navigation pane on the left, choose **NAT Gateway > Private NAT Gateways**.
4. Configure required parameters. For details, see [Table 4-6](#).

**Table 4-6** Parameter descriptions of a transit IP address

| Parameter          | Description   |
|--------------------|---|
| Transit VPC        | VPC to which the transit IP address is located  |
| Transit Subnet     | A transit subnet is a transit network and is the subnet to which the transit IP address belongs.<br>The subnet must have at least one available IP address.   |
| Transit IP Address | The transit IP address can be assigned in either of the following ways:<br><b>Automatic:</b> The system automatically assigns a transit IP address.<br><b>Manual:</b> You need to manually assign a transit IP address. |
| IP Address         | This parameter is only available when you set <b>Transit IP Address</b> to <b>Manual</b> .  |

5. Click **OK**.

## 4.7.2 Viewing a Transit IP Address

### Scenarios

View details about transit IP addresses assigned to you.

### Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.  
The NAT gateway console is displayed.
3. In the navigation pane on the left, choose **NAT Gateway > Private NAT Gateways**.
4. Click the **Transit IP Addresses** tab and then click the transit IP address.
5. On the page displayed, view details about the assigned transit IP addresses.

## 4.7.3 Releasing a Transit IP Address

### Scenarios

Release a transit IP address that you no longer need.

### Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner. Under **Network**, select **NAT Gateway**.  
The NAT gateway console is displayed.
3. In the navigation pane on the left, choose **NAT Gateway > Private NAT Gateways**.
4. In the **Transit IP Addresses** area, locate the transit IP address you want to release, and click **Release** in the **Operation** column.
5. Click **Yes**.

#### NOTE

If a transit IP address has been associated with an SNAT or DNAT rule, it cannot be released. To release such a transit IP address, delete all rules associated with it first.

## 4.8 Accessing On-Premises Data Centers or Other VPCs

### Accessing On-Premises Data Centers

You can use Direct Connect or VPN to connect the transit VPC to your on-premises data centers.

For a higher quality connection, use Direct Connect. For details, see *Direct Connect User Guide*.

For more cost-effective connectivity, use VPN. For details, see *Virtual Private Network User Guide*

## Accessing Other VPCs

You can use VPC Peering to connect the transit VPC to other VPCs.

For details, see *Virtual Private Cloud User Guide*.

# 5 Permissions Management

---

## 5.1 Creating a User and Granting NAT Gateway Permissions

This section describes how to use IAM to implement fine-grained permissions control for your NAT Gateway resources. With IAM, you can:

- Create IAM users for employees based on your enterprise's organizational structure. Each IAM user will have their own security credentials for accessing NAT Gateway resources.
- Grant only the permissions required for users to perform a specific task.
- Entrust an account or cloud service to perform efficient O&M on your NAT Gateway resources.

If your account does not require individual IAM users, skip this section.

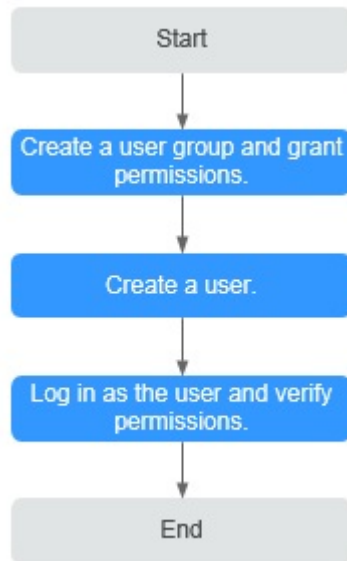
This section describes the procedure for granting permissions (see [Figure 5-1](#)).

### Prerequisites

Learn about the permissions supported by NAT Gateway and choose policies or roles according to your requirements. For details, see [Permissions Management](#). For the permissions of other services, see [System Permissions](#).

## Process Flow

**Figure 5-1** Process for granting NAT Gateway permissions



1. Create and authorize a user group.  
Create a user group on the IAM console, and attach the **ReadOnlyAccess** policy to the group.
2. Create an IAM user and add it to a user group.  
Create a user on the IAM console and add the user to the group created in **1**.
3. Log in and verify permissions.  
Log in to the management console as the created user. Switch to the authorized region and verify the permissions.
  - Choose **Service List > NAT Gateway**. Then click **Create NAT Gateway**. If a message appears indicating that you have insufficient permissions to perform the operation, the **ReadOnlyAccess** policy has already taken effect.
  - Choose any other service in **Service List**. If a message appears indicating that you have insufficient permissions to access the service, the **ReadOnlyAccess** policy has already taken effect.

## 5.2 NAT Gateway Custom Policies

You can create custom policies to supplement system-defined policies of NAT Gateway. For the actions that can be added to custom policies, see section "Permissions Policies and Supported Actions" in *NAT Gateway API Reference*.

To create a custom policy, choose either visual editor or JSON.

- Visual editor: Select cloud services, actions, resources, and request conditions. You do not need to have knowledge of the policy syntax.
- JSON: Create a JSON policy or edit an existing one.

For operation details, see section "Creating a Custom Policy" in *Identity and Access Management User Guide*. The following section contains examples of common NAT Gateway custom policies.

## Example Policies

- Example 1: Grant permissions to create and delete a NAT gateway.

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "nat:natGateways:create",
        "nat:natGateways:delete"
      ]
    }
  ]
}
```

- Example 2: Grant permission to deny NAT gateway deletion.

A policy with only "Deny" permissions must be used together with other policies. If the permissions assigned to a user contain both "Allow" and "Deny", the "Deny" permissions take precedence over the "Allow" permissions.

The following method can be used if you need to assign permissions of the NAT Gateway **FullAccess** policy to a user but also forbid the user from deleting NAT gateways. Create a custom policy for denying NAT gateway deletion, and attach both policies to the group to which the user belongs. Then the user can perform all operations on NAT gateways except deleting NAT gateways. The following is an example of a deny policy:

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Action": [
        "nat:natGateways:delete"
      ],
      "Effect": "Deny"
    }
  ]
}
```

- Example 3: Defining permissions for multiple services in a policy

A custom policy can contain actions of multiple services that are of the global or project-level type. The following is an example policy containing actions of multiple services:

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Action": [
        "nat:natGateways:update",
        "nat:natGateways:create"
      ],
      "Effect": "Allow"
    },
    {
      "Action": [
        "vpc:vpcs:update"
      ],
      "Effect": "Allow"
    }
  ]
}
```

```
]
}
```

# 6 Monitoring

## 6.1 Supported Metrics

### Description

This section describes metrics reported by NAT Gateway to Cloud Eye as well as their namespaces, monitoring metrics, and dimensions. You can use the management console or the APIs provided by Cloud Eye to query the metrics generated for NAT Gateway.

### Namespace

SYS.NAT

### Metrics

**Table 6-1** NAT Gateway metrics

| Metric ID             | Name                         | Description   | Value Range | Monitored Object | Monitoring Period (Raw Data) |
|-----------------------|------------------------------|---|-------------|------------------|------------------------------|
| snat_connection       | SNAT Connections             | Number of SNAT connections of the NAT gateway<br>Unit: count                            | $\geq 0$    | NAT gateway      | 1 minute                     |
| Server IP address set | Monitoring Details of Top 10 | IP addresses of the top 10 servers that occupy the most SNAT connections<br>Unit: count | $\geq 0$    | NAT gateway      | 1 minute                     |



**Table 6-2** Private NAT gateway metrics

| Metric ID          | Name               | Description  | Value Range    | Monitored Object    | Monitoring Period (Raw Data) |
|--------------------|--------------------|--|----------------|---------------------|------------------------------|
| snat_connection    | SNAT Connections   | Number of SNAT connections of the NAT gateway<br>Unit: count         | $\geq 0$       | Private NAT gateway | 1 minute                     |
| inbound_bandwidth  | Inbound Bandwidth  | Inbound bandwidth of servers using the SNAT function<br>Unit: bit/s  | $\geq 0$ bit/s | Private NAT gateway | 1 minute                     |
| outbound_bandwidth | Outbound Bandwidth | Outbound bandwidth of servers using the SNAT function<br>Unit: bit/s | $\geq 0$ bit/s | Private NAT gateway | 1 minute                     |
| inbound_pps        | Inbound PPS        | Inbound PPS of servers using the SNAT function<br>Unit: count        | $\geq 0$       | Private NAT gateway | 1 minute                     |
| outbound_pps       | Outbound PPS       | Outbound PPS of servers using the SNAT function<br>Unit: count       | $\geq 0$       | Private NAT gateway | 1 minute                     |

| Metric ID        | Name             | Description   | Value Range | Monitored Object    | Monitoring Period (Raw Data) |
|------------------|------------------|---|-------------|---------------------|------------------------------|
| inbound_traffic  | Inbound Traffic  | Inbound traffic of servers using the SNAT function<br>Unit: byte  | ≥ 0 bytes   | Private NAT gateway | 1 minute                     |
| outbound_traffic | Outbound Traffic | Outbound traffic of servers using the SNAT function<br>Unit: byte | ≥ 0 bytes   | Private NAT gateway | 1 minute                     |

## Dimensions

| Key                | Value                  |
|--------------------|------------------------|
| nat_gateway_id     | Public NAT gateway ID  |
| vpc_nat_gateway_id | Private NAT gateway ID |

## 6.2 Viewing Metrics

### Prerequisites

- The NAT gateway is running properly and SNAT rules have been created.
- It can take a period of time to obtain and transfer the monitoring data. Therefore, wait for a while and then check the data.

### Scenarios

This section describes how to view NAT Gateway metrics.

### Procedure

1. Log in to the management console.
2. In the upper left corner, select the target region.
3. Under **Management & Deployment**, select **Cloud Eye**.

4. In the navigation pane on the left, choose **Cloud Service Monitoring > NAT Gateway**.
5. Locate the row that contains the target metric and click **View Metric** in the **Operation** column to check detailed information.

You can view data of the last one, three, or twelve hours.

# 7 FAQs

---

## 7.1 Public NAT Gateways

### 7.1.1 What Is the Relationship Between a VPC, Public NAT Gateway, EIP Bandwidth, and ECS?

- A VPC is a secure, isolated, logical network environment.
- A public NAT gateway enables ECSs in a VPC to access the Internet.
- EIP is a service that provides valid static IP addresses on the Internet. The throughput of a VPC is determined by the EIP bandwidth.
- An ECS is an instance running in a VPC and uses a public NAT gateway to access the Internet.

### 7.1.2 How Does a Public NAT Gateway Offer High Availability?

The backend of a public NAT gateway supports automatic disaster recovery through hot standby, thereby reducing risks and improving availability.


## 7.2 Private NAT Gateways

### 7.2.1 How Do I Troubleshoot a Network Failure After a Private NAT Gateway Is Configured?


#### Checking Security Group Rules

If the traffic to and from the ECS port is denied in the security group, add rules to the security group to allow the port traffic.

**Step 1** Log in to the management console.

- Step 2** Click  in the upper left corner and select the desired region and project.
- Step 3** Under **Compute**, select **Elastic Cloud Server**.
- Step 4** In the ECS list, click the name of the ECS for which you will check the security group rules.
- Step 5** Click the **Security Groups** tab and view security group rules.
- Step 6** Check whether you have configured inbound and outbound rules to allow traffic to and from the ECS port.
- If yes, go to [Checking Whether Default Route Pointing to the Private NAT Gateway Is Configured in the Route Table](#).
  - If no, go to [Step 7](#).
- Step 7** Click **Manage Rule**. On the displayed page, click **Inbound Rules** or **Outbound Rules** to add an inbound rule and outbound rule that allow traffic to and from the ECS port.
- End

## Checking Whether Default Route Pointing to the Private NAT Gateway Is Configured in the Route Table

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select the desired region and project.
- Step 3** Under **Networking**, click **Virtual Private Cloud**.
- Step 4** In the navigation pane on the left, choose **Route Tables**.
- Step 5** In the route table list, click the name of the route table associated with the VPC to which the private NAT gateway belongs.
- Step 6** Check whether the route pointing to the private NAT gateway is configured in the route list.
- End

## 7.2.2 How Many Private NAT Gateways Can I Create in a VPC?

You can create a maximum of 10 private NAT gateways in a VPC.

## 7.2.3 Can an SNAT Rule and a DNAT Rule of a Private NAT Gateway Share the Same Transit IP Address?

No.

## 7.2.4 Can Private NAT Gateways Translate On-premises IP Addresses Connected to the Cloud Through Direct Connect?

Yes. When you are creating a DNAT rule and select **Custom** for **Instance Type**, you can add an on-premises IP address.

## 7.2.5 What Are the Differences Between Private NAT Gateways and Public NAT Gateways?

Private NAT gateways perform NAT between private IP addresses and resolve the following problems:

- Private IP address conflicts
- Access from specified addresses

Public NAT gateways perform NAT between private IP addresses and public IP addresses and have the following advantages:

- Secure: Only shared EIPs, instead of all EIPs of servers, are exposed to the Internet.
- Cost-effective: EIPs and bandwidth are shared, saving network infrastructure costs.

## 7.2.6 Can a Private NAT Gateway Be Used Across Accounts?

Private NAT gateways cannot be used across accounts. However, you can use a VPC peering connection to connect transit VPCs of the two accounts. In this way, the two VPCs where the private NAT gateways of the two accounts are deployed can communicate with each other.

## 7.3 SNAT Rules

### 7.3.1 Why Do I Need SNAT?

**Public NAT gateways:** Besides requiring services provided by the system, some ECSs also need to access the Internet to obtain information or download software. However, assigning a public IP address to each ECS consumes already-limited IPv4 addresses, incurs additional costs, and may increase the attack surface in a virtual environment. Enabling multiple ECSs to share a public IP address is preferable and more practical. This can be done using SNAT.

**Private NAT gateways:** Different departments of a large enterprise may have a large number of overlapping CIDR blocks. After the enterprise migrates its workloads to the cloud, those departments will not be able to communicate with each other. In this case, SNAT can be used to translate the IP addresses of multiple ECSs in a department into a transit IP address for accessing other departments. In other scenarios where high security is required, an industry regulation agency may require other organizations to use a specified IP address to access the regulation system. In this case, SNAT can translate the IP addresses of multiple servers in an organization to one transit IP address, that is, the specified IP address.

### 7.3.2 What Are SNAT Connections?

An SNAT connection consists of a source IP address, source port, destination IP address, destination port, and a transport layer protocol. An SNAT connection uniquely identifies a session. The source IP address and source port refer to the IP address and port after NAT.

SNAT supports three protocols: TCP, UDP, and ICMP. A NAT gateway supports up to 55,000 concurrent connections to each destination IP address and port. If any of the destination IP address, port number, and protocol (TCP, UDP, or ICMP) changes, you can create another 55,000 connections. The number of connections you query on an ECS may be different from the actual number of SNAT connections. (You can run the **netstat** command to query the number of connections.) Assume that an ECS creates 100 connections to a fixed destination every second. 55,000 connections will be used up in about 10 minutes without considering the dropped idle connections. As a result, new connections cannot be established.

If there is no data packet passing through the SNAT connection for a long time, the connection will be timed out.

## 7.4 DNAT Rules

### 7.4.1 Why Do I Need DNAT?

In a public NAT gateway, DNAT enables servers in a VPC to share an EIP to provide services accessible from the Internet. With an EIP, a public NAT gateway forwards the Internet requests from only a specific port and over a specific protocol to a specific port of a server, or it can forward all requests to the server regardless of which port they originated on. For details, see [Adding a DNAT Rule](#).

In a private NAT gateway, DNAT enables servers that share the same transit IP address in a VPC to provide services accessible from on-premises data centers or other VPCs. For details, see section "Adding a DNAT Rule" under "Managing Private NAT Gateways" in *NAT Gateway User Guide*.

### 7.4.2 Can I Modify DNAT Rules?

You can modify DNAT rules. For public and private NAT gateways, DNAT rules can be modified.

---

# A Change History

---

| Released On | Description                               |
|-------------|---|
| 2024-04-15  | This issue is the first official release. |